FACULTAD DE CIENCIAS JURÍDICAS | upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa | ZIENTZIA JURIDIKOEN FAKULTATEA

TRABAJO FIN DE MÁSTER / MASTER
AMAIERAKO LANA

INVESTIGACIÓN Y PRUEBA DEL HECHO ELECTRÓNICO EN EL PROCESO

Unai Urtasun Villabona

DIRECTOR / ZUZENDARIA

Manuel Richard González

Pamplona / Iruñea

4 de junio de 2021 / 2021eko ekainaren 4a

RESUMEN Y PALABRAS CLAVE

La amplia integración de las TICs en cada uno de los ámbitos de la realidad social hace que no en pocas ocasiones, cada vez más, tengamos la necesidad de probar hechos electrónicos en el proceso judicial. Por este motivo, el presente trabajo tiene por objeto clarificar determinadas ideas, como qué ha de entenderse por hecho electrónico, al tiempo que se estudia y expone la forma en que ha de producirse la investigación y obtención de la prueba del hecho electrónico, los medios probatorios por los que se aportará al proceso y las reglas que rigen la valoración de la prueba. Así pues, en contra de lo que generalmente cabría esperar, se concluye que el hecho electrónico se acreditará de forma semejante al resto de hechos.

Hecho electrónico; prueba; investigación y obtención de la prueba; proceso; derecho fundamental.

ABSTRACT AND KEY WORDS

The wide integration of ICTs in each of the areas of social reality means that not infrequently, more and more, we have the need to prove electronic facts in the judicial process. For this reason, the present project seeks to clarify certain ideas, such as what is meant by an electronic fact, while exploring and explaining the manner in which the investigation and taking of evidence of an electronic fact is to take place, the means of proof by which it is to be used and the rules governing the evaluation of evidence. Thus, contrary to what might generally be expected, it is concluded that the electronic fact will be credited in a similar way to the other facts.

Electronic fact; proof; investigation and obtaining of evidence; process; fundamental right.

LABURPENA ETA HITZ GAKOAK

IKTak gizarte-errealitatearen eremu bakoitzean erabat integratuta dauden heinean, prozesu judizialean, gero eta gehiago, gertakari elektronikoak frogatu behar izaten ditugu. Hori dela eta, lan honen xedea ideia jakin batzuk argitzea da, hala nola zer ulertu behar den gertakari elektronikotzat, eta, aldi berean, lan honen bitartez aztertu eta azaldu egiten da nola ikertu eta lortu behar den gertakari elektronikoaren froga, zein froga-baliabideren bidez lagunduko den prozesuan eta zein diren probaren balorazioa arautzen duten arauak. Beraz, oro har espero zitekeenaren kontra, ondorioztatzen da gertakari elektronikoa gainerako gertakarien antzera egiaztatuko dela.

Gertaera elektronikoa; froga; ikerketa eta frogaren eskuratzea; prozesu; oinarrizko eskubidea.

ABREVIATURAS

CC	Código Civil
CE	Constitución española de 1978
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
DRAE	Diccionario de la Real Academia Española
ET	Estatuto de los Trabajadores
IMAP	*Internet Message Access Protocol*
IMSI	*International Mobile Suscriber Identity*
IMEI	*International Mobile Equipment Identity*
IP	*Internet Protocol*
LAJ	Letrado de la Administración de Justicia
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LFE	Ley de firma electrónica
LOPDGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica del Poder Judicial
LN	Ley del Notariado
LRJS	Ley Reguladora de la Jurisdicción Social

Núm.	Número
Ob. cit.	Obra citada
Pág./Págs.	Página/Páginas
POP3	*Post Office Protocol revision 3*
RGPD	Reglamento General de Protección de Datos
RN	Reglamento Notarial
SMS	*Short Message Service*
SMSC	*Short Message Service Center*
SMTP	*Simple Mail Transfer Protocol*
TC	Tribunal Constitucional
TICs	Tecnologías de la información y comunicación
TSJ	Tribunal Superior de Justicia

ÍNDICE

I INTRODUCCIÓN

Las nuevas tecnologías de la información y comunicación (o TICs) han transformado notablemente la forma en que se producen o se manifiestan los hechos en la realidad social contemporánea. Ello es así en la medida en que hemos pasado a comunicarnos y relacionarnos con otras personas por medio del correo electrónico, del WhatsApp o de las redes sociales; trabajamos con un correo electrónico corporativo asignado por la empresa y tenemos acceso a grandes cantidades de archivos y datos almacenados de forma electrónica; compramos, contratamos y negociamos electrónicamente y, por supuesto, cometemos delitos a través de instrumentos informáticos o de cualquiera de las TICs. Sin olvidar el cambio que se ha producido en la forma en que nos relacionamos con la administración pública, ya sea para tramitar la solicitud de una beca, para pedir una cita en el medico, una prestación de la Seguridad Social o en el ámbito tributario.

Como no podría ser de otra forma, el derecho procesal y los procesos judiciales no son ajenos a los cambios que se producen en la realidad social y, con una mayor o menor actualización de las leyes procesales, han tenido que adaptarse a la nueva coyuntura. Un ejemplo de este proceso de adaptación lo constituyen las nuevas medidas de investigación tecnológica introducidas por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Al mismo tiempo, como forma de entender y explicar este contexto marcado por la revolución tecnológica, la doctrina ha creado el concepto de la "prueba electrónica" sobre el que existe discusión en cuanto a su existencia o naturaleza.

Asimismo, se hace imprescindible aclarar los criterios y métodos que han de seguirse en la investigación y obtención de la prueba de los hechos electrónicos o de las manifestaciones de hechos producidas en medios electrónicos, dado el riesgo existente de superar los límites fijados por los derechos fundamentales y de la consiguiente declaración del carácter ilícito de la prueba. Acto seguido, resulta esencial conocer el medio probatorio idóneo para aportar la prueba del hecho electrónico al proceso, atendiendo para ello a la regulación de los medios de prueba y a los distintos pronunciamientos judiciales habidos al respecto. Finalmente, será fundamental conocer cuál es la eficacia probatoria del medio o conjunto de medios de prueba aportados y las

circunstancias que influyen en la convicción del órgano judicial y que redundan una mayor o menor fuerza probatoria.

En pocas palabras, el propósito de este trabajo no es otro que aclarar ciertas ideas básicas y explicar la forma en que debe llevarse a cabo la investigación y obtención, la prueba y la valoración del hecho electrónico.

II CUESTIONES PREVIAS DE LA MATERIA OBJETO DE ESTUDIO

1. Caracteres del hecho electrónico

El hecho electrónico es un hecho social y, por tanto, un hecho susceptible de aportación al proceso, de prueba y de valoración. RICHARD GONZÁLEZ lo define de forma concisa señalando que los hechos electrónicos «*son hechos que tienen relación con la electrónica ya sea por su origen o por su tratamiento técnico*»[1]. De este modo, el hecho electrónico es un hecho relacionado mediata o inmediatamente con la electrónica, es decir, tiene relación con dispositivos que utilizan la electrónica. Por ello, son hechos que se manifiestan de algún modo con la intervención de procesos y dispositivos electrónicos[2].

La calificación de un hecho como electrónico no lo hace diferente del resto de hechos en general, de modo que el hecho electrónico no estará sujeto a exigencias legales distintas a efectos de conseguir su introducción en el proceso jurisdiccional y tampoco en cuanto a su valoración.

A este efecto es, por lo general, intrascendente la génesis y origen de los hechos que se manifiestan de forma electrónica. Así, ciertamente y en sentido estricto podríamos definir como hechos electrónicos tanto las ondas electromagnéticas de radiofrecuencia que posibilitan la comunicación entre personas como las que modulan

[1] RICHARD GONZÁLEZ, M. "Análisis crítico sobre la naturaleza y características de la prueba pericial electrónica en el proceso jurisdiccional", en *Revista Jurídica de Catalunya-Aranzadi*, 2017, pág. 17.

[2] Es un hecho relacionado con los electrones, que son partículas con carga eléctrica negativa que giran alrededor del núcleo del átomo, formando parte de la estructura atómica de la materia; y con la electrónica, que se refiere al «*estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos*», según la definición que de dicho concepto recoge el Diccionario de la Lengua Española de la Real Academia Española (en adelante, DRAE). A este respecto, cabe señalar que con carácter general los dispositivos electrónicos emplean semiconductores para controlar los electrones, pues estos componentes son capaces de resistir, transportar, seleccionar, dirigir, conmutar, almacenar, manipular y explotar el electrón.

la frecuencia de la emisora de radio que escuchamos, los programas informáticos, el conjunto de pixeles y datos que conforman los archivos de texto, imagen, sonido o video con una extensión determinada (.doc, .pdf, .jpg, .gif,…), etc. Pero, al final lo que resulta de interés es el modo en el que la tecnología ofrece hechos que pueden ser captados por nuestros sentidos ya sea mediante impresiones en papel, información ofrecida en pantallas de video, etc. Esto es, información aprehensible para el ser humano, en forma de señales de luz, sonido o pixeles en una pantalla. Esto se consigue a través del uso de la tecnología que permite la generación y transmisión de ideas y datos de cualquier clase mediante el uso dispositivos, *softwares* especializados o máquinas o dispositivos técnicos (*hardware*)[3]. Nótese que sin la intermediación técnica de traducción del lenguaje binario de las máquinas al lenguaje humano la información relativa al hecho electrónico no sería comprensible ni susceptible de tratamiento por las personas. Lo mismo sucede con las comunicaciones telefónicas, dado que en estas el teléfono móvil actúa como receptor y transmisor de ondas electromagnéticas de radiofrecuencia. Así, las ondas sonoras de la voz del emisor se convierten en ondas electromagnéticas que, una vez alcanzan el teléfono móvil del destinatario, se transforman de nuevo en sonido para que el mensaje pueda escucharse y comprenderse.

2. Principales medios electrónicos en los que se producen los hechos

Existe una gran heterogeneidad dentro de los hechos producidos a través de medios electrónicos como consecuencia del constante avance de la tecnología. Es por ello que el presente apartado se va a centrar en el análisis de aquellos medios electrónicos que con mayor habitualidad aparecen en la práctica jurídica ante los Tribunales.

2.1 El documento electrónico

En virtud de lo dispuesto en el artículo 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE), se considera documento electrónico la «*información de cualquier naturaleza en forma electrónica, archivada en un soporte*

[3] El *software* se refiere al código y/o programa que contiene el conjunto de instrucciones que sigue el ordenador, ejemplo de ello serían aplicaciones como Microsoft Word u Open Office, sistemas operativos como Windows o Android y navegadores de internet como Explorer o Google Chrome. El *hardware*, sin embargo, hace referencia a los componentes físicos de un ordenador, es decir, es la estructura física que permite a la persona interactuar con el ordenador. Así pues, pueden mencionarse a modo de ejemplo el monitor, el ratón, el disco duro, la memoria USB, la memoria RAM, el procesador, etc.

electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado»[4]. Dentro de este concepto pueden incluirse, además de los documentos de texto u hojas de cálculo, facturas electrónicas, las imágenes digitalizadas (incluidos los "pantallazos"), ficheros de sonido, videos digitalizados o un registro o conjunto de registros dentro de una base de datos, y otros muchos[5]. En lo relativo al proceso penal, el artículo 26 CP determina que «*a los efectos de este Código se considera documento todo soporte material que exprese e incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*».

Por su parte, ABEL LLUCH, enumera y explica cuáles serían los elementos del documento electrónico[6]:

1) Soporte: se corresponde con el objeto que puede llevarse a presencia del órgano judicial para ser analizado en el proceso, y que podrá ser magnético, óptico, un pendrive, un disco duro u otros nuevos dispositivos que pudieran crearse.
2) Contenido: entendiéndose como la representación de un hecho o acto jurídico, en el documento electrónico, en contra de lo sucede con el documento escrito, puede diferenciarse entre el contenido y la forma de presentación. Ello es así por cuanto la información grabada el lenguaje binario precisa de la ayuda de instrumentos informáticos para que sea inteligible y pueda ser apreciada por el Juzgador. De esta forma, la forma de representación se refiere a los medios de reproducción mediante los cuales se exterioriza (programas de software), que a su vez emplean elementos auxiliares (PCs, teléfonos inteligentes, tabletas, etc.) para mostrar su contenido de forma legible y apta para surtir efectos en el proceso.
3) Autor: frente al documento escrito tradicional, en el que puede conocerse el autor del mismo a través de la firma o de las características grafológicas en caso de ser manuscrito, en el documento electrónico puede resultar algo más

[4] Por su parte, ILLAN FERNÁNDEZ señala que son documentos electrónicos «*todos aquellos objetos materiales en los que puede percibirse una manifestación de voluntad o representativos de un hecho de interés para el proceso que pueda obtenerse a través de los modernos medios reproductivos, como la fotografía, la fonografía, la cinematografía, el magnetófono, las cintas de vídeo, los discos de ordenador y cualesquiera otros similares*», en ILLAN FERNÁNDEZ, J.M., *La prueba electrónica, eficacia y valoración en el proceso civil. Nueva oficina judicial, comunicaciones telemáticas (Lexnet) y el expediente judicial electrónico. Análisis comparado legislativo y jurisprudencial.* Aranzadi, Navarra, 2009, pág. 467.

[5] De acuerdo con el DRAE, se entiende por "pantallazo" la «*captura del contenido que se visualiza en la pantalla de una computadora u otro dispositivo electrónico*».

[6] ABEL LLUCH, X. Y PICÓ I JUNOY, J. *La prueba electrónica. Colección de Formación Continua Facultad de Derecho ESADE.* J.M. Bosch editor, Barcelona, 2011, págs. 37-40.

complejo conocer la persona que hay detrás del mismo. Sucede pues que en muchas ocasiones podrá llegar a conocerse el dispositivo concreto mediante el cual se creó un archivo determinado pero no la persona que lo confecciono, a no ser que el mismo venga acompañado de una firma electrónica que dé certeza de su autoría[7].

4) Fecha y firma: la fecha del documento electrónico es un elemento que en la mayoría de las veces se agrega automáticamente por el propio programa empleado para su creación, si bien es cierto que resulta un elemento fácilmente manipulable por el usuario a través de los ajustes de la aplicación. Respecto de la firma de documentos electrónicos, habrá que atender a las disposiciones de la LFE que posibilitan, en determinadas ocasiones, acreditar qué persona o entidad ha creado un determinado documento.

Dentro de esta clase de medio electrónico, cabe apreciar las siguientes modalidades: — 1º el documento electrónico público, — 2º el documento electrónico "oficial" y — 3º el documento electrónico privado[8]. Estos tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable (artículo 3.7 LFE).

La primera modalidad se corresponde con el documento firmado electrónicamente por fedatario público, encontrándose dentro de esta categoría los siguientes tipos:

---

[7] Atendiendo a lo dispuesto en la LFE podemos diferenciar entre dos tipos de firma electrónica que serán la firma electrónica avanzada y la firma electrónica reconocida, definiéndose por la propia ley en los apartados segundo y tercero del artículo 3 de la siguiente forma:
«*2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.*
3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma».
Por otro lado, en lo que concierne a la firma electrónica reconocida, el apartado cuarto del mismo artículo le concede el mismo valor que el que tiene la firma manuscrita en relación con los datos consignados en papel.

[8] Así lo señala el artículo 3.6 de la LFE cuando afirma que: «*El documento electrónico será soporte de:*
a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.
b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.
c) Documentos privados».

1) Documentos públicos judiciales, refiriéndose estos a las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Letrados de la Administración de Justicia (artículo 317.1º LEC).
2) Documentos públicos notariales, esto es, los autorizados por notario con arreglo a derecho (artículo 317.2º LEC).
3) Documentos públicos administrativos u oficiales, que son aquellos que provienen de los Secretarios y otros funcionarios con facultad certificante de las Administraciones Públicas, con respecto a los actos administrativos de éstas (artículo 317.3º a 6º LEC)[9].

La segunda de las modalidades, el documento electrónico "oficial", hace referencia, según lo dispuesto en el artículo 3.6.b LFE, a los «*documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica*».

La última de las modalidades referidas, el documento electrónico privado, se define de forma negativa al estar identificado con los documentos que no puedan ser incluidos en las categorías de documento público o de documento oficial. En este sentido, la sentencia del Tribunal Supremo de 08/07/2011, núm. de recurso 6115/2007, señala tajantemente que «*Sólo gozan de la consideración de documentos públicos los indicados en el artículo 317 de la LEC siendo los demás documentos de carácter privado, por el principio de exclusión (artículo 324 de la LEC)*».

[9] Artículo 317 LEC (Clases de documentos públicos): «*A efectos de prueba en el proceso, se consideran documentos públicos:*
1.º Las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Letrados de la Administración de Justicia.
2.º Los autorizados por notario con arreglo a derecho.
3.º Los intervenidos por Corredores de Comercio Colegiados y las certificaciones de las operaciones en que hubiesen intervenido, expedidas por ellos con referencia al Libro Registro que deben llevar conforme a derecho.
4.º Las certificaciones que expidan los Registradores de la Propiedad y Mercantiles de los asientos registrales.
5.º Los expedidos por funcionarios públicos legalmente facultados para dar fe en lo que se refiere al ejercicio de sus funciones.
6.º Los que, con referencia a archivos y registros de órganos del Estado, de las Administraciones públicas o de otras entidades de Derecho público, sean expedidos por funcionarios facultados para dar fe de disposiciones y actuaciones de aquellos órganos, Administraciones o entidades».

2.2 Correo electrónico

De conformidad con el artículo 2 h) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), se entiende por correo electrónico «*todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo*».

El esquema de funcionamiento de esta forma de comunicación puede sintetizarse de la siguiente forma[10]:

- Es un sistema que permite el intercambio de mensajes entre distintos ordenadores o dispositivos móviles interconectados a través de internet, para lo cual se emplea la dirección electrónica del remitente estableciendo como receptora otra u otras direcciones electrónicas conocidas por este.
- Funciona como un sistema de cliente/servidor: cuando el emisor envía un correo, su cliente se conecta a un servidor SMTP, este recibe la orden de entregar un correo y procede a consultar en el servidor DNS a qué buzón de correo o servidor debe entregarlo[11]. A continuación el servidor SMTP se pondrá en contacto con el servidor receptor, que empleará una conexión POP3 o IMAP para entregar el correo[12]. Finalmente, el receptor del correo utilizará también un programa de correo electrónico para acceder al mensaje.
- El análisis del correo electrónico requiere de la investigación y examen de dos bloques de información; por un lado, el contenido del mensaje y los diferentes contenidos digitales que se hayan podido adjuntar con él, y, por otro lado, los

[10] DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Wolters Kluwer, Madrid, 2016, pág. 167-168.

[11] El SMTP (*Simple Mail Transfer Protocol* o protocolo simple de transferencia de correo) es un protocolo de mensajería utilizado para enviar un correo (o email) de un servidor de origen a otro de destino.

[12] IMAP (*Internet Message Access Protocol*) y POP3 (*Post Office Protocol revision 3*) son dos métodos para acceder al correo electrónico, siendo el IMAP el más empleado. El POP3 descarga los mensajes en el ordenador eliminándolos del servidor, lo que significa que en caso de acceder al correo electrónico desde otro ordenador o dispositivos los mensajes que se hayan descargado anteriormente no se encontraran disponibles; por el contrario, el IMAP permite consultar los correos en más de un dispositivo y en cualquier momento porque estos se hayan en el servidor del correo electrónico, es decir, en este caso no se descargan ni almacenan en el dispositivo.

datos de tráfico que hacen referencia, por ejemplo, a la fecha y hora del correo y al origen y destino del mismo[13].

- La estructura básica de cualquier correo electrónico se compone de los siguientes elementos básicos: el destinatario (que puede ser uno concreto o varias personas, existiendo la posibilidad de que las direcciones que se van a incluir no sean visibles para el resto de personas), el asunto (cuya finalidad es enunciar de forma concisa el tema o finalidad del correo) y el mensaje (siendo posible una configuración personal del tipo de letra, color, alineación, etc.), así como los archivos adjuntos que pueden ser de diversa tipología (textos, hojas de cálculo, fotografías, videos, etc.).
- Cuando el usuario desea acceder a su cuenta de correo electrónico, antes de poder enviar mensajes o leer los recibidos ha de introducir una contraseña o *password* que garantiza la privacidad de su contenido y, en cierta medida, la identidad de la persona que utiliza dicha cuenta.

Asimismo, resulta necesario señalar que, de acuerdo con la definición de correo electrónico ofrecida por el artículo 2 h) de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, se entiende que los SMS se encuentran dentro de esta modalidad de medio electrónico[14]. El SMS (*Short Message Service*) es un servicio que permite a los titulares de teléfonos móviles enviar mensajes cortos de texto

[13] Véase FERNÁNDEZ RODRÍGUEZ, J.J. "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, 108, 93-122.doi: http://dx.doi.org/10.18042/cepc/redc.108.03, en que se aporta información relevante a este respecto: «*Los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje4. Son un subproducto de las conexiones, que se concretará en función del tipo de comunicación. Así, en una llamada telefónica, se trata del número de teléfono de llamada, el nombre y la dirección del abonado de origen, el número de destino y el nombre y dirección del abonado de destino, la fecha y hora del comienzo y fin de la comunicación, el servicio telefónico utilizado, y otros datos específicos de la telefonía móvil (la identidad internacional del abonado [lMSI] que llama y del que recibe la llamada; la identidad internacional del equipo móvil [IMEI], también del que llama y del que recibe la llamada; si el servicio es de pago por adelantado: fecha y hora de la primera activación del servicio y la etiqueta de localización o identificador de celda desde la que se haya activado el servicio). En cambio, en el acceso a internet y en el correo electrónico serán metadatos, tanto para el origen como para el destino de la comunicación, la identificación de usuario asignada, el nombre y la dirección del abonado o usuario al que se le ha atribuido una dirección de protocolo internet (IP); la fecha y hora de conexión y desconexión del servicio de acceso a internet; el servicio de internet utilizado; o la línea digital de abonado (DSL). Téngase en cuenta que la dirección del protocolo internet puede ser dinámica o estática, en función de la asignación que realiza el proveedor de acceso. Estamos incluyendo parte de los datos de localización en los datos de tráfico, porque son tratados en la conducción de una comunicación*».

[14] «*Además, a efectos de la presente Directiva se entenderá por: […] h) «correo electrónico»: todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo*».

y que, igualmente, permite el envío de pequeños archivos de sonido o de imágenes. Cuando se envía un SMS, el teléfono móvil lo remite automáticamente al servidor del operador del usuario, conocido como SMSC (*Short Message Service Center*), el cual lo reenvía al destinatario, que se identifica introduciendo el número del teléfono móvil de la persona a la que se quiere remitir el mensaje. De esta forma, se trata de una comunicación realizada a través de un canal cerrado, en el que los datos se envían a través de un servidor.

2.3 Sistemas de mensajería instantánea: WhatsApp

Para conocer la importancia del Whatsapp en la realidad social actual, resulta muy ilustrativa la encuesta sobre el «*Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares*» realizada en el año 2020 por el Instituto Nacional de Estadística[15]. En ella se observa como el uso de servicios de mensajería instantánea como WhatsApp es la actividad más realizada (por el 89,5% de la personas de 16 a 74 años y por el 22% de las personas mayores de 75 años)[16]. Le siguen la búsqueda de información sobre bienes y servicios en el caso de las personas de 16 a 74 años (78,3%) y telefonear o realizar videollamadas a través de Internet en el caso de los mayores de 74 años (16,6%).

La aplicación para smartphones WhatsApp es una plataforma de mensajería instantánea que posibilita la comunicación mediante mensajes de texto entre sus usuarios, al tiempo que permite el envío de fotografías, videos, archivos, notas de audio e incluso contactos guardados en la agenda del teléfono móvil y la ubicación del propio dispositivo (en un momento determinado o en tiempo real). Además, esta aplicación se encuentra disponible en multiplataforma: Android, IOS, Windows Phone y BlackBerry OS.

En lo que respecta al ámbito técnico y de seguridad de la comunicación, WhatsApp Messenger emplea un sistema de cifrado de extremo a extremo (o *end-to-end*) que garantiza que únicamente el emisor y el receptor del mensaje puedan leerlo o

[15] Instituto Nacional de Estadística. (2020). *Instituto Nacional de Estadística*. Madrid: INE. Recuperado de https://www.ine.es/prensa/tich_2020.pdf

[16] Ello tiene repercusiones en todos los ámbitos, incluido el familiar, en el que el uso indebido de esta aplicación, para insultar e injuriar, ha motivado sentencias condenatorias por lesión del derecho al honor junto con la condena a indemnizar por los daños y perjuicios causados (sentencia de la Audiencia Provincial de Barcelona de 17/09/2020, núm. 614/2020, Aranzadi).

escucharlo. De esta forma, cada mensaje tiene su propio candado y solamente el emisor y el receptor tienen el código o la llave necesaria para poder leer o escuchar el mismo. A mayor abundamiento, la compañía WhatsApp Inc. tampoco tiene la posibilidad de acceder a los mensajes de sus usuarios puesto que estos no se guardan en ningún servidor de propiedad de la empresa, sino que se almacenan en los propios terminales de los usuarios. Por ello, cuando un usuario de la aplicación envía un mensaje, aunque el mismo pase por los servidores de la compañía que lo procesan y reenvían a su destinatario, una vez el mensaje ha sido recibido y descargado por el destinatario, el servidor automáticamente procede a eliminarlo.

Si bien es cierto que este sistema garantiza de forma fiable la seguridad de las comunicaciones, también lo es que ha recibido críticas en la medida en que imposibilita la interceptación de las comunicaciones, previa autorización judicial, por parte de los Cuerpos y Fuerzas de Seguridad del Estado. De hecho, ni el antiguo SITEL ni el actual sistema Evident X-Stream empleado por el Ministerio del Interior pueden acceder al contenido cifrado.

2.4 Las redes sociales

En una primera aproximación teórica al universo de las redes sociales, el DRAE ofrece una sencilla definición, señalando que una red social consiste en una «*plataforma digital de comunicación global que pone en contacto a gran número de usuarios*»[17].

Partiendo de la anterior definición, es necesario aludir a la existencia de diferentes tipos de redes sociales que pueden concretarse principalmente en dos tipos: las horizontales, que ostentan un carácter generalista y que se encuentran integradas por usuarios sin características o intereses específicos que mediante la creación de perfiles personales publican contenidos e interactúan entre sí (Facebook, Twitter,…); y las verticales, que se corresponden con aquellas redes sociales especializadas dirigidas a usuarios con un perfil específico y un interés común (redes profesionales como

[17] De forma más completa y extensa, el Diccionario Panhispánico del Español Jurídico define la red social como el *«servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios del grupo».*

Linkedin, redes de música como Myspace,…). Al mismo tiempo, cabe diferenciar entre las redes sociales públicas y privadas, encontrándose las primeras disponibles para todo tipo de usuarios y las segundas solamente para los miembros de un grupo u organización privada; y las redes sociales directas (que pueden ser horizontales y verticales) e indirectas (blogs y foros).

En cuanto a la prueba del hecho electrónico en esta área, en ocasiones habrá que probar unos hechos que hayan tenido lugar en redes sociales, y en otras ocasiones la información que estas albergan servirá como elemento probatorio de un hecho no cometido en redes sociales. Así, en relación al proceso que pueda llegar a sustanciarse en cualquier orden jurisdiccional, la información contenida en un perfil abierto de una red social puede ser de entidad suficiente como para constituir un importante elemento probatorio.

De esta forma, dentro del ámbito penal, por ejemplo, cabe mencionar el delito de quebrantamiento de una prohibición de comunicación producida en la red social Facebook (sentencia de la Audiencia Provincial de Madrid de 20/11/2017, núm. 291/2017) o el delito de enaltecimiento del terrorismo producido en la red social Twitter (sentencia del Tribunal Supremo de 07/05/2020, núm. 135/2020)[18]. Mientras que en el ámbito laboral, por ejemplo, cabe destacar los supuestos de despido disciplinario del trabajador debido a los insultos y faltas de respeto vertidos en redes sociales (Twitter en este caso) contra la empresa y compañeros de trabajo, superando los límites de la libertad de expresión (sentencia del Tribunal Superior de Justicia de Madrid de 19/07/2019, núm. 804/2019); así como los supuestos de despido disciplinario por la transgresión de la buena fe contractual al realizar el trabajador, como podía observarse en sus redes sociales, trabajos incompatibles con la situación de incapacidad temporal (sentencia del Tribunal Superior de Justicia de Madrid de 05/05/2017, núm. 313/2017).

2.5 Las páginas web

El elemento fundamental a tener en cuenta cuando se pretenda probar un hecho o hechos que hayan tenido lugar en una página web, es el carácter cambiante de estas. Esto se materializa en una constante actualización de su contenido, que puede llevar a

[18] Para más información acerca del papel que están jugando los *tweets* en el proceso penal véase BUENO DE MATA, F. Y GONZÁLEZ PULIDO, I. *Fodertics 7.0. Estudios sobre derecho digital*. Editorial Comares, Granada, 2019, págs. 269-277.

que en un determinado momento la página web en cuestión deje de mostrar aquello que interese a la estrategia procesal de parte (al igual que sucede en las redes sociales). Por tanto, una forma diligente de actuar será acudir lo antes posible ante un notario o Letrado de la Administración de Justicia para que de fe pública del contenido existente en una fecha determinada y en una concreta página web con una específica URL. No obstante, también cabe la posibilidad de solicitar el reconocimiento judicial para que el órgano judicial aprecie por sí mismo el contenido de la página web.

De igual modo, con el objeto de solventar este carácter cambiante de las páginas web, las partes tienen la posibilidad de acudir a los conocidos como Terceros de Confianza (*Trusted Third Party* o *TTP*) o Prestadores de Servicios de Confianza Digital[19] .

Finalmente, en cuanto a supuestos reales en que lo sucedido en una determinada página web ha sido determinante para la resolución del caso, cabe mencionar la sentencia de Tribunal Supremo de 08/05/2019, núm. 347/2019. En este caso, tras declarase acreditada la publicación de unos comunicados relativos a la actividad sindical de CNT en la página web de la empresa, la Sala declaró producida una lesión al derecho a la libertad sindical del referido sindicato con motivo del contenido de dichas comunicaciones.

3. Distinción entre hechos y medios de prueba

El hecho se configura como un elemento meta jurídico, extrajurídico o a-jurídico, que necesariamente se corresponde con una realidad previa y ajena al proceso judicial. De este modo, existirá con independencia de que se inicie o no el proceso, y, en tanto en cuanto éste no se inicie, el hecho por sí mismo carecerá de repercusiones jurídicas. Por tanto, el hecho es un elemento de naturaleza material, es decir, se trata del testimonio de las partes o testigos en relación a lo acontecido, de los documentos, del conocimiento técnico, científico o artístico del perito, de un elemento real objeto de examen que, como se ha dicho, existen de forma previa e independiente al proceso.

[19] Véanse DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital…*, ob. cit., 2016, págs. 95-97; y GUARDIOLA SALMERÓN, M. (2018). ¿Cómo recabar y aportar la prueba digital? *Derecho & Perspectiva*, págs. 1-6. Recuperado de http://derechoyperspectiva.es/como-recabar-y-aportar-la-prueba-digital/

Por contra, los medios de prueba se configuran, por un lado, como los actos procesales que sirven para que las partes acrediten los hechos en el proceso y, por otro lado, como los instrumentos procesales a partir de los cuales el Juzgador adquiere conocimiento de los hechos. Por lo tanto, el medio de prueba es un elemento de naturaleza procesal, esto es, existe dentro del proceso.

Junto con la distinción previamente realizada, se ha de precisar que mientras que los hechos son fruto de la realidad y, por tanto, tienen tantas formas y lo son en tanto número como en cada caso se precise, esto es, que no están sujetos a una lista cerrada, los medios de prueba se reducen a los tasados en el artículo 299 LEC, sin perjuicio de una reforma legal al respecto[20].

En este sentido, la rápida evolución tecnológica y el empleo masivo de los instrumentos electrónicos en todos los ámbitos de la vida social, hacen que los posibles hechos producidos a través de medios electrónicos se hayan incrementado considerablemente. En las últimas dos décadas se ha visto como la variedad de instrumentos informáticos, multimedia y/o de comunicaciones ha ido creciendo, al tiempo que lo han hecho los formatos y soportes empleados: teléfonos móviles, smartphones (con sistema operativo IOS, Android y otros), tabletas, ordenadores, dispositivos USB, unidades ZIP, Cd-Rom, DVD, reproductores de MP3 o MP4, servidores de información, el cloud computing, PDAs, navegadores, pantallas táctiles en automóviles, etc. Esta gran variedad de fuentes probatorias ha de tener acceso al proceso a través un soporte determinado, lo que determinará el medio de prueba utilizado, siendo, en principio, todos los medios de prueba legalmente previstos aptos para incorporar al proceso los datos recogidos a través de medios electrónicos.

De igual modo, ha de tenerse en cuenta que en el mismo proceso pueden emplearse varios medios probatorios de forma cumulativa, por ejemplo, mediante la aportación del teléfono móvil en el que se encuentre una conversación mantenida en una aplicación de mensajería instantánea (como WhatsApp o Telegram), junto a una transcripción escrita de la misma solicitando el cotejo por el Letrado de la

[20] Artículo 299.1 LEC: *«Los medios de prueba de que se podrá hacer uso en juicio son: 1.º Interrogatorio de las partes. 2.º Documentos públicos. 3.º Documentos privados. 4.º Dictamen de peritos. 5.º Reconocimiento judicial. 6.º Interrogatorio de testigos».*

Administración de Justicia; y la testifical (o interrogatorio de parte) acerca del contenido de dicha conversación.

En definitiva, las diferentes modalidades de hechos producidos a través de medios electrónicos que vayan surgiendo, deben aportarse al proceso a través del medio de prueba que más se ajuste a sus particularidades.

4. Delimitación conceptual de la prueba electrónica y debate doctrinal sobre su existencia

La prueba constituye el elemento esencial de nuestro proceso judicial en la medida en que el resultado de su práctica determinará el convencimiento del juez en relación a los hechos controvertidos alegados por las partes, y, por tanto, la realidad fáctica sobre la que va a operar la norma jurídica y que traerá consigo la estimación o desestimación de sus pretensiones. De esta forma, la prueba se erige como aquella actividad de parte dirigida a convencer al juez de la veracidad de unos hechos que se afirma que han tenido lugar en la realidad. No obstante, lo cierto es que el término prueba viene siendo empleado no solamente para hacer alusión a la actividad probatoria, sino también para hacer referencia al resultado de esta actividad y al medio mediante el cual se logra dicho resultado.

El objeto de la prueba vendrá referido a los hechos controvertidos alegados por las partes en sus respectivos escritos de demanda y contestación y, en su caso, aquellos que se introduzcan posteriormente de acuerdo con las normas procesales de cada orden jurisdiccional. Ahora bien, no todos los hechos son susceptibles de ser alegados, dado que solamente lo serán aquellos que guarden relación con el debate procesal (pertinencia) y contribuyan a esclarecer los hechos controvertidos (utilidad). Así, por ejemplo, no será necesario probar hechos notorios o aquellos respecto de los cuales exista plena conformidad de las partes, salvo en los casos en que la materia objeto del proceso esté fuera del poder de disposición de los litigantes (artículo 281.3 y 4 LEC).

Como se observará a continuación, la doctrina emplea múltiples denominaciones para referirse a la prueba electrónica objeto de estudio en el presente apartado. Entre estas, la terminología más común es la que alude a la "prueba electrónica", pero se han venido utilizando asimismo los conceptos de "prueba tecnológica", "prueba

informática", "prueba telemática", "prueba cibernética", "prueba digital" o "prueba del hecho virtual". Dichos términos no pueden considerarse como sinónimos entre sí, lo cual hace necesario cuanto menos un conciso ejercicio de diferenciación.

De esta forma, empezando por el término que más habitualmente es empleado, el DRAE define el adjetivo "electrónico" como «*perteneciente o relativo a la electrónica; o que funciona mediante la electrónica*». En cuanto a otros términos de uso habitual, el DRAE define los conceptos "informática" y "tecnológica" haciendo referencia el primero al «*conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras*», y, el segundo, que es el término escogido en las últimas reformas procesales habidas sobre la materia, a lo «*perteneciente o relativo a la tecnología*»[21].

Otro de los vocablos que vienen siendo empleados por la doctrina, en concreto, el relativo a la prueba "cibernética", es definido por el DRAE como «*perteneciente o relativo a la cibernética; creado y regulado mediante computadora o perteneciente o relativo a la realidad virtual*». Por este motivo, esta expresión se refiere, fundamentalmente, a la actividad relacionada con las redes telemáticas (ya sean abiertas, cerradas o de acceso restringido), quedando los sistemas informáticos como instrumentales o secundarios.

El término "telemática", por su parte, proviene de la combinación de los vocablos "telecomunicaciones" e "informática", siendo los elementos telemáticos los que hacen posible el establecimiento de vínculos comunicativos a larga distancia a través de internet. El DRAE conceptualiza lo telemático como lo «*perteneciente o relativo a la telemática*» y como la «*aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada*»[22].

Los dos términos anteriores son, quizás, los que más diferencias presentan con relación al resto, y se refieren a aquellas pruebas que tienen su origen en la aplicación de nuevas tecnologías vinculadas a alguna red de comunicación (red local o Internet).

[21] Esto es, lo perteneciente o relativo al "*conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento*" o también el "*conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto*", quedando la prueba tecnológica circunscrita al empleo de instrumentos o procedimientos técnicos.

[22] Por tanto, se incluyen dentro de dicho término, la comunicación oral, de imágenes o datos producida mediante diversos dispositivos como, por ejemplo, ordenadores o tablets.

Por otro lado, la conocida como "prueba del hecho virtual", solamente hace alusión a los hechos relacionados con las nuevas tecnologías, no incluyendo, por tanto, aquellas investigaciones que, llevadas a cabo mediante el empleo de las nuevas tecnologías, aportan hechos que pueden no ser perteneciente a aquellos.

Finalmente, el término "digital", según el DRAE, hace referencia a «*un dispositivo o sistema: Que crea, presenta, transporta o almacena información mediante la combinación de bits*».

A diferencia de lo que sucede en los hechos no electrónicos, en los hechos electrónicos existe una serie de información conocida como "metadatos". Dicho término proviene del griego "μετα" (después de) y de "data" plural del latín datum –i (datos), lo cual literalmente significa "más allá de los datos", haciendo referencia a aquellos datos que definen o describen otros datos, como, por ejemplo: la fecha de su creación o modificación, el autor de los mismos, o incluso la cámara empleada cuando se trata de una fotografía. Los metadatos, en definitiva, son un conjunto de datos ocultos que se graban en forma de ceros y unos en una unidad de almacenamiento y que necesitan ser transformados en un contenido legible para que las partes y el tribunal conozcan su alcance y contenido.

Hecha estas previas y concisas aclaraciones, y con ánimo de determinar que se entiende por prueba electrónica, procede traer a colación las definiciones ofrecidas por distintos autores. Para SANCHÍS CRESPO la prueba electrónica o en soporte electrónico es aquella a través de la cual se adquiere el conocimiento de un hecho controvertido a raíz de la información contenida en un dispositivo electrónico, ya sea mediante el convencimiento psicológico, o fijando un determinado hecho como cierto de conformidad con una norma legal[23].

ARRABAL PLATERO, por su parte, señala que la prueba tecnológica se refiere, por un lado, a los datos informáticos con transcendencia en un proceso judicial (poniendo como ejemplo los contenidos en un pen drive o un disco duro) y, por otro lado, a aquellos elementos que han sido obtenidos mediante el empleo de medios tecnológicos

[23] SANCHÍS CRESPO, C. *La prueba en soporte electrónico*, en VALERO TORRIJOS, J. (coord.), *Las tecnologías de la información y la comunicación en la administración de justicia : análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, Navarra, 2012, pág. 713.

(como sucede, por ejemplo, con el peritaje informático, las comunicaciones interceptadas por medio de mecanismos tecnológicos,...).

DELGADO MARTÍN, de forma más breve, señala que por prueba digital o electrónica cabe entender «*toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio*»[24]. Seguidamente, procede a destacar los siguientes elementos en relación a dicha definición:

1) Se alude a cualquier clase de información;
2) Información que ha de ser producida, almacenada o transmitida por medios electrónicos[25].
3) Dicha información debe tener la capacidad de acreditar hechos en el proceso tramitado dentro de cualquier orden jurisdiccional. En lo que concierne al ámbito penal, ha de tenerse en cuenta que puede servir para la investigación de todo tipo de infracciones penales y no se encuentra limitada a los denominados delitos informáticos.

La doctrina que aboga por la existencia de la prueba electrónica se divide entre quienes entienden que se constituye como una prueba autónoma que debe regularse como un medio de prueba específico, los que entienden que se trata de una prueba ya regulada en el artículo 299.2 LEC, y, finalmente, aquellos que defienden que se trata de una especialidad de la prueba documental.

En sentido contrario, RICHARD GONZÁLEZ opina que el ordenamiento jurídico procesal no recoge ninguna norma que pueda corresponderse con una eventual prueba electrónica. Entiende que la misma no viene recogida en el primer apartado del artículo 299 LEC, pero que tampoco puede entenderse incluida dentro de los apartados segundo y tercero, identificando lo dispuesto por el apartado segundo como un medio de prueba autónomo o complementario de los establecidos en el primer párrafo, y lo dispuesto en el apartado tercero simplemente como una norma cierre del sistema de medios de

[24] DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital…, ob. cit.,* 2016, págs. 42-43.
[25] En el Anexo de definiciones de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, se determina que se entenderá por medio electrónico todo «*Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras*».

prueba[26]. Igualmente, niega categóricamente lo que por algunos se ha denominado prueba documental electrónica, señalando que el documento electrónico es un concepto sustantivo que se incorporará al proceso mediante una impresión de texto, de imagen o de video, y cuando su contenido no sea directamente entendible mediante prueba pericial, en este caso, informática o tecnológica.

En este sentido, el autor explica que cada uno de los medios de prueba se relaciona con actividades que permiten la activación de los sentidos y que, de esta manera, proporcionan información al cerebro del juzgador con la finalidad de convencerle de que dicte sentencia en uno u otro sentido. Dicho en sus propios términos, «*los medios de prueba están relacionados directamente con nuestra dotación biológica como especie que nos ha provisto de varios sentidos, que no son sino canales de comunicación con nuestro entendimiento como animales sociales (con nuestro cerebro en definitiva): vista, tacto, oído, gusto y olfato*»[27]. Dicho esto, continua su explicación afirmando que por la mayor o menor precisión de cada uno de los sentidos, así como por los usos y convenciones sociales, se discrimina entre ellos siendo plenamente utilizados como canales del medio de prueba únicamente la vista y el oído (testifical, interrogatorio y documental). El resto de los sentidos, o bien son empleados escasamente, como es el caso del tacto y el olfato (reconocimiento judicial), o bien no juegan ningún papel en el sistema de medios de prueba, como es el caso del gusto. Por consiguiente, la prueba se construye como un acto humano, lo que hace inviable hablar de probar un hecho electrónico o no mediante prueba electrónica.

Bajo esta lógica, el autor concluye que todo lo que trascienda de nuestros sentidos, como, por ejemplo, datos digitales o radiaciones electromagnéticas, deberá probarse mediante prueba pericial. Por ello, en caso de que se hable de prueba electrónica, esta se debería ubicar dentro de la prueba pericial y, en concreto, como una prueba pericial tecnológica o informática que sirva para conocer los detalles técnicos del

[26] Artículo 299.2 y 3 LEC:
2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.
3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.
[27] RICHARD GONZÁLEZ, M. "Análisis crítico sobre…", ob. cit., 2017, pág. 9.

hecho electrónico que no son directamente aprehensibles por las personas, sin que por ello pierda su naturaleza de prueba pericial.

III LA PRUEBA DE LOS HECHOS PRODUCIDOS A TRAVÉS MEDIOS ELECTRÓNICOS EN EL PROCESO JUDICIAL

1. Investigación y Obtención de la prueba del hecho electrónico

1.1 La afectación de determinados derechos fundamentales en la fase de investigación y obtención de la prueba

Los derechos examinados en los siguientes apartados gozan de un amplio reconocimiento tanto a nivel interno, mediante su inclusión como derechos fundamentales en el artículo 18 CE, como a nivel internacional en instrumentos como la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, el Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966, el Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950 y la Carta de Derechos Fundamentales de la Unión Europea. De hecho, de acuerdo con el artículo 10.2 CE, los anteriores textos internacionales constituyen los parámetros de acuerdo a los cuales se deberán interpretar los derechos fundamentales y las libertades públicas reconocidas por la Constitución.

1.1.1 Derecho fundamental a la intimidad personal y familiar

La protección de la intimidad personal y familiar viene amparada por el artículo 18.1 CE que recoge este derecho fundamental en un sentido amplio junto con los derechos fundamentales al honor y a la propia imagen.

La doctrina del Tribunal Constitucional ha tratado de delimitar los contornos del derecho fundamental a la intimidad que se regula de un modo poco concreto en el artículo 18.1 CE. A este respecto entiende el TC que el derecho a la intimidad garantiza un ámbito reservado de la vida del individuo vedando que sean terceros, particulares o poderes públicos, quienes decidan cuáles han de ser los límites de nuestra vida privada[28]. Siendo así se entiende que cada persona tiene el derecho de reservarse

[28] Véase en cuanto al alcance de este derecho fundamental ARRABAL PLATERO, P. *La prueba tecnológica: aportación, práctica y valoración.* Tirant lo Blanch, Valencia, 2020, págs. 121-125.

un espacio protegido de la curiosidad ajena, sea cual sea el contenido de ese espacio[29]. De esta forma, como señala la sentencia del Tribunal Constitucional de 09/05/2013, núm. 115-2013, de la existencia de este derecho deviene la correlativa obligación de toda persona de abstenerse de cualquier intromisión en la esfera íntima del resto y la prohibición de hacer uso de lo así conocido.

La doctrina sobre la expectativa razonable de privacidad, relacionada con los actos de las personas, se ha construido sobre la delimitación del área que cada individuo reserva para sí mismo o para su familia. Según esta doctrina, cuando el individuo, de manera voluntaria y/o consciente, participa en actividades o actúa de forma que sus actos quedan expuestos al conocimiento o escrutinio público, no habrá intromisión ilegítima en su intimidad. Esto será así en la medida en que no cabe deducir una voluntad de reserva por parte del mismo[30].

Los datos o informaciones contenidos en dispositivos electrónicos (documentos, fotografías, vídeos,…), así como los datos de navegación en la web (qué se busca, cuándo, con qué frecuencia,…), forman parte del derecho fundamental a la intimidad personal y familiar en tanto en cuanto se refieren a datos perfectamente aptos para crear un perfil personal altamente descriptivo de la esfera íntima y de la personalidad del individuo. Por tanto, a efectos de evitar la ilicitud de la prueba y su nulidad, el acceso a estos datos o la obtención de los mismos debe producirse de acuerdo con las garantías que legitiman la injerencia en este derecho fundamental. En este sentido, desde una óptica constitucional, la injerencia en el derecho a la intimidad tendrá una justificación objetiva y razonable cuando se cumpla con los siguientes requisitos (sentencia del Tribunal Constitucional del 07/11/2011, núm. 173/2011): la existencia de un fin constitucionalmente legítimo, como lo son el interés público propio de la prevención e investigación del delito y, en concreto, la determinación de los hechos relevantes para el

[29] A este respecto, a modo de ejemplo, la sentencia del Tribunal Supremo de 19/04/2017, núm. 287/2017 (Aranzadi) dice lo siguiente: *«Y es que, frente a lo que sucede respecto del contenido material de otros derechos, el derecho a la intimidad o, si se quiere, el espacio de exclusión que frente a otros protege el derecho al entorno virtual, es susceptible de ampliación o reducción por el propio titular. Quien incorpora fotografías o documentos digitales a un dispositivo de almacenamiento masivo compartido por varios es consciente de que la frontera que define los límites entre lo íntimo y lo susceptible de conocimiento por terceros, se difumina de forma inevitable»*.

[30] En relación con esta doctrina de la expectativa razonable de privacidad, cabe mencionar las sentencias del Tribunal Constitucional de 30/01/2012, núm.12/2012 (Aranzadi) y de 28/02/2019, núm. 25/2019 (Aranzadi) que declaran lo siguiente: «*una conversación mantenida en un lugar específicamente ordenado a asegurar la discreción de lo hablado, como ocurre por ejemplo en el despacho donde se realizan las consultas profesionales, pertenece al ámbito de la intimidad*».

proceso penal; que la medida limitativa del derecho este prevista en la ley (principio de legalidad); que como regla general se acuerde mediante resolución judicial motivada y, por último, la estricta observancia del principio de proporcionalidad que, a su vez, se concreta en tres condiciones: idoneidad y necesidad de la medida y juicio de proporcionalidad en sentido estricto.

Por el contrario, el individuo no se verá amparado por ninguna clase de reserva o protección constitucional con relación a los datos que difunda por internet en canales o ámbitos no restringidos. Siendo así, se entiende que el titular de los datos presta un consentimiento tácito que posibilita el conocimiento de dicha información por parte de terceras personas.

1.1.2 Derecho fundamental al secreto de las comunicaciones

Recogido en el artículo 18.3 CE, este derecho fundamental determina la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas y, por tanto, esta obligación negativa se extiende a todo tercero ajeno a la comunicación ya sean particulares o agentes públicos. Así pues, se observa una doble dimensión dentro de este derecho fundamental referida, de un lado, al proceso de comunicación en sí mismo, y, de otro lado, al contenido del mensaje transmitido con independencia de que este sea banal o de interés público, puesto que, a diferencia del derecho a la intimidad, el derecho al secreto de las comunicaciones es un derecho de carácter formal. Como consecuencia de lo anterior, sucede que si bien toda comunicación (de unas ciertas características) es secreta, no todo el contenido de los mensajes intercambiados en la misma tiene porqué ser íntimo.

DELGADO MARTÍN en un análisis de lo que se entiende por proceso de comunicación distingue tres elementos básicos: — 1º la transmisión de información o contenido; — 2º a que la misma se produzca entre dos o más personas determinadas o determinables, siendo titulares de este derecho las personas físicas o jurídicas nacionales

o extranjeras[31]; y — 3º la intermediación de un tercero prestador del servicio de comunicación unido a los interlocutores por vínculos de confidencialidad[32].

En cuanto al primero, el autor subraya la característica de la integridad que supone, como ya se ha adelantado, la protección de todo tipo de comunicaciones con independencia de su contenido o de su representación en forma de signos (sonidos, señales, caracteres, emoticonos, etc.), realizadas por cualquier canal o medio de transmisión, abarcando los datos externos de la comunicación también conocidos como los datos de tráfico asociados a la comunicación[33]-[34]. Dichos datos, atendiendo a la definición otorgada por el artículo 1.d) del Convenio sobre Ciberdelincuencia de Budapest, otorgan información sobre el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente. Por otro lado, el artículo 588 ter b.2.3º LECrim, en el ámbito de la interceptación de comunicaciones telefónicas y telemáticas, afirma que *«se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga»*. Por ello, este derecho se verá afectado por la eventual entrega de las listas de llamadas telefónicas por parte de las compañías telefónicas o por el acceso al registro de llamadas entrantes y salientes de un teléfono móvil, en tanto en cuanto permiten la identificación subjetiva de los interlocutores (sentencia del Tribunal Constitucional de 02/07/2012, núm. 142/2012). Sin embargo, no toda información que pueda obtenerse de un dispositivo electrónico

[31] Incluyéndose las personas físicas menores de edad de acuerdo con lo previsto en el artículo 4.1 LO 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

[32] DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital…, ob. cit.*, 2016, págs. 112-116.

[33] Como señala la sentencia del Tribunal Constitucional de 09/10/2006, núm. 281/2006 (Aranzadi): «*Varias precisiones son aún necesarias a los efectos de la delimitación de la noción constitucional de correspondencia del art. 18.3 CE. De un lado, en la medida en que los mensajes pueden expresarse no sólo mediante palabras, sino a través de otro conjunto de signos o señales que componen otra clase de lenguajes, y dado que los mensajes pueden plasmarse no sólo en papel escrito, sino también en otros soportes que los incorporan –cintas de cassette o de vídeo, CD's o DVD's, etc., – la noción de correspondencia no puede quedar circunscrita a la correspondencia escrita, entendida ésta en su sentido tradicional*».

[34] Esta inclusión dentro del ámbito protegido del artículo 18.3 CE se observa, a nivel interno, en las sentencias del Tribunal Constitucional de 29/11/1984, núm. 114/1984 (Aranzadi) o de 02/07/2012, núm. 142/2012 (Aranzadi), así como a nivel europeo en las sentencias del Tribunal Europeo de Derechos Humanos de 02/08/1984, Caso Malone contra Reino Unido y de 03/04/2007, Caso Copland contra Reino Unido.

que sea apto o este diseñado para llevar a cabo procesos comunicativos afecta al secreto de las comunicaciones[35].

Con relación al segundo de los elementos, sirviendo de ejemplo las comunicaciones producidas en redes sociales, habrá que diferenciar los supuesto en que los usuarios comparten información con un número reducido de destinatarios en comunidades de acceso restringido y los casos en que la información es de acceso público (blogs, Twitter,...). En este último supuesto, no existirá proceso de comunicación y no quedará protegido por el secreto de las comunicaciones.

La relevancia del tercer y último elemento se halla en que la protección que dispensa este derecho fundamental no alcanza a todos los fenómenos de comunicación existentes entre personas, sino que únicamente protege las comunicaciones que se realizan a través de determinados medios o canales cerrados. En este sentido, el autor ofrece varios ejemplos de comunicaciones abiertas que quedarían fuera del ámbito de protección de este derecho: las comunicaciones radiofónicas, las que tienen lugar en circuitos electrónicos cerrados como porteros automáticos o interfonos, y las formas de envió de la correspondencia que legalmente se configuran como una comunicación abierta[36].

Igualmente, se ha planteado la necesidad de delimitar qué fases del proceso de comunicación, la fase previa al inicio del proceso de comunicación, el momento en que la comunicación se está produciendo o se encuentra vigente y la fase final en la que el proceso comunicativo ha terminado, se hallan protegidas por el secreto de las

[35] Como se advierte en esta misma sentencia, el acceso de los agentes de la Guardia Civil, sin consentimiento del titular del teléfono móvil ni autorización judicial, a la agenda de contactos telefónicos, no comporta ningún tipo de afectación al secreto de las comunicaciones en la medida en que no se trata de datos que formen parte de una comunicación actual o consumada, y tampoco proporciona información alguna acerca de actos concretos de comunicación pretéritos o futuros. Así, se afirma que a efectos de delimitar el contenido de los derechos fundamentales recogidos en los artículos 18.1 y 18.3 CE, lo determinante no es el soporte, físico o electrónico, en que está alojada la agenda de contactos, sino el carácter de la información a la que se accede. De esta forma, en este caso el derecho fundamental afectado sería el derecho a la intimidad. Un caso similar al expuesto se recoge en la sentencia del Tribunal Constitucional de 09/05/2013, núm. 115/2013 (Aranzadi).

[36] Como recoge la sentencia del Tribunal Constitucional de 09/10/2006, núm. 281/2006 (Aranzadi): *«Desde esta perspectiva, no gozan de la protección constitucional aquellos objetos –continentes– que por sus propias características no son usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías (ATC 395/2003, de 11 de diciembre, F. 3), de modo que la introducción en ellos de mensajes no modificará su régimen de protección constitucional. Ni tampoco gozan de la protección constitucional del art. 18.3 CE aquellos objetos que, pudiendo contener correspondencia, sin embargo, la regulación legal prohíbe su inclusión en ellos, pues la utilización del servicio comporta la aceptación de las condiciones del mismo».*

comunicaciones. Cuando el proceso de comunicación no se ha iniciado, la jurisprudencia ha entendido que el acceso al contenido de mensajes no enviados no afecta al secreto de las comunicaciones. De modo que la interceptación de un paquete postal con anterioridad a que sea depositado en las oficinas postales no implicará una injerencia en el secreto de las comunicaciones precisamente por no haberse iniciado el proceso comunicativo[37]. Lo mismo cabría decir de aquellos mensajes de correo electrónico que se encuentran en la carpeta de borradores.

Ahora bien, cuando se trate de acceder al contenido de una comunicación en curso, ello indudablemente supondrá la afectación del derecho al secreto de las comunicaciones, ya sea en el caso de que el mensaje haya sido enviado y recibido sin que su destinario lo haya leído o abierto, o en el caso de que el mensaje se encuentre técnicamente en proceso de transmisión. Por el contrario, una vez el proceso de comunicación se haya consumado, es decir, una vez el mensaje se haya enviado, recibido y leído, como ya no existe proceso de comunicación el derecho al secreto de las comunicaciones no se verá afectado por el acceso a la información de dicho mensaje almacenado en el dispositivo electrónico, en un servidor o, en su caso, que se halle en soporte físico, aunque sí el derecho a la intimidad[38]. A este respecto, VEGAS TORRES considera que la forma de dilucidar si se ha vulnerado el secreto de las comunicaciones radica en determinar si el acceso u obtención de los datos de la comunicación se ha producido con interferencia o sin interferencia de la comunicación[39]. De este modo, el secreto de las comunicaciones se verá afectado cuando en la obtención de los datos haya mediado una interferencia del proceso comunicativo, con independencia de que el acceso a la información tenga lugar una vez concluida la comunicación. Sin embargo, no se verá afectado este derecho cuando se acceda a los datos sin que medie una interferencia en el proceso de comunicación, con independencia de que el acceso a los datos se produzca antes o después de finalizar la comunicación.

En relación con la idea anterior, procede pasar a analizar aquellas situaciones en las que se puede entender afectado el derecho al secreto de las comunicaciones y

[37] Véase la sentencia del Tribunal Constitucional de 03/06/2002, núm. 137/2002 (Aranzadi) (FJ 3º), como ejemplo de un supuesto en el que se entendió que no hubo interceptación de ninguna comunicación.
[38] Véanse a este respecto las sentencias del Tribunal Constitucional de 03/04/2002, núm. 70/2002 (FJ 9º) y de 07/11/2011, núm. 173/2011 (FJ 3º) (Aranzadi).
[39] VEGAS TORRES, J. *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*. Universidad Rey Juan Carlos, Madrid, 2011, pág. 62.

aquellas otras en que, por el contrario, no entrará en juego la protección otorgada por este derecho que, como sabemos, no es de alcance absoluto. Así, el alcance de este derecho dependerá de que las comunicaciones se produzcan a través de un canal abierto o cerrado, así como de las circunstancias de la persona que obtiene la información para su posterior incorporación al proceso, es decir, si se trata de una de las personas que participó en el proceso de comunicación o de un tercero ajeno a la comunicación.

En relación al canal por el que se produzca la comunicación, como ya se ha comentado, las comunicaciones protegidas por el secreto de las comunicaciones serán aquellas comunicaciones cerradas que tengan lugar, por ejemplo, a través de un medio postal, telefónico, fax, electrónico o mensajería instantánea. Por consiguiente, los individuos no se verán amparados por este derecho fundamental en las comunicaciones directas con otras personas ni en las comunicaciones dirigidas o accesibles a un número indeterminado de personas, como sucede en el caso de las redes sociales.

En cuanto a las circunstancias de la persona que accede a la información, la jurisprudencia entiende que el secreto de las comunicaciones no alcanza a la persona que haya formado parte del proceso de comunicación y, por tanto, este derecho no se entenderá vulnerado por el acceso o por el empleo que esta persona haga de la información nacida del proceso comunicativo. Todo ello, sin perjuicio de una posible vulneración del derecho a la intimidad como consecuencia del uso que pueda darse a dicha información, siempre y cuando se trate de información que afecte a aspectos de la esfera íntima del otro interlocutor (o interlocutores, en su caso, cuando participen más de dos personas en la comunicación)[40]. De este modo lo ha venido reflejando la jurisprudencia tanto del Tribunal Constitucional como del Tribunal Supremo a partir de la sentencia del Tribunal Constitucional de 29/11/1984, núm. 114/1984. Dicha sentencia señala que el núcleo esencial de este derecho se encuentra en la interdicción de cualquier penetración en la comunicación por parte de terceros ajenos a la misma, lo cual no se produce por la divulgación o comunicación de aquella por parte de alguno de los interlocutores, dado que estos no vienen obligados a guardar secreto de la conversación producida entre ambos (sin perjuicio de lo señalado sobre el derecho a la intimidad).

[40] Por ejemplo, los e-mails con varios destinatarios.

En una reciente sentencia de la Audiencia Provincial de Alicante, el tribunal desestima la petición de nulidad por vulneración del derecho al secreto de las comunicaciones respecto de un archivo sonoro reproducido en el acto del juicio, el cual había sido obtenido por el hermano del querellante al grabar un trascendental acto asambleario en el que participó, ello pese a la expresa prohibición de grabar el acto que existía en aquel momento[41]. En este caso, tomando como base la jurisprudencia del Tribunal Constitucional previamente citada, la audiencia entiende que no se ha grabado una conversación ajena, sino que se trataba un acto al que acudió y en el que participó la persona que realizó la grabación, con independencia de la prohibición de grabar el acto.

Como puede inferirse, la única forma legítima y compatible con el derecho al secreto de las comunicaciones de interceptar una comunicación o de acceder al contenido de la misma será mediante autorización judicial[42]. Esta autorización deberá ser solicitada por la autoridad pública competente en el ejercicio del *ius puniendi* del Estado o en el marco de procesos concursales, debiendo someterse al control judicial la medida que en su caso pueda adoptarse. En este caso, el auto del juez de Instrucción que autorice la intervención lo hará con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, y deberá estar lo suficientemente motivado con base a una investigación en curso y ponderando, de acuerdo con el artículo 588 bis a.5 LECrim, la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho fundamental[43].

---

[41] Sentencia de la Audiencia Provincial de Alicante de 10/04/2019, núm. 142/2019 (Aranzadi).

[42] La sentencia de la Audiencia Provincial de Madrid de 01/10/2012, núm. 1260/2012 (Aranzadi), confirma la actuación de la policía en contra de lo alegado por la defensa que entendía vulnerado el artículo 18.3 CE por el acceso de los agentes a los mensajes de WhatsApp del acusado: *«Pero tal intervención operó previa autorización judicial llevada a cabo por auto del Magistrado del Juzgado de Instrucción de 29 de septiembre de 2011 .*
Así, mediante oficio de 28 de septiembre de 2011 el Equipo de Policía Judicial de la Jefatura del Servicios Fiscal y Aeroportuario de la Guardia Civil remitió oficio al Juzgado de Instrucción número 51 de Madrid (folio 75) en el que, además de dar cuenta de las investigaciones realizadas, se solicitó autorización judicial para el encendido del terminal telefónico móvil que portaba don Elias en el momento de su detención, marca APPLE modelo IPHONE A1332 con nº IMEI NUM016 , al objeto de comprobar y reseñar datos sobre comunicaciones vía SMS, MMS, datos de Internet móvil (WhatsApp) y datos de contactos de la agenda telefónica. […]Por lo tanto, la injerencia en tal comunicación, previa autorización judicial, es legítima y por lo tanto, sin vulneración "ilegítima" de los derechos fundamentales, por lo que no cabe apreciar causa de nulidad y consideramos que tales elementos probatorios son válidos, lícitos y legítimos, susceptibles de plena valoración a la hora de enjuiciar los hechos objeto de acusación».

[43] En ocasiones, como señala la sentencia del Tribunal Supremo de 04/12/2015, núm. 786/2015 (Aranzadi), será posible hacerlo mediante providencia: *«En palabras de la STC 123/2002, 20 de mayo*

1.1.3 Derecho fundamental a la protección de datos

El derecho fundamental a la protección de datos del artículo 18.4 CE, también denominado derecho a la autodeterminación informativa o *habeas data*, es un derecho fundamental autónomo que, en ocasiones, ha sido confundido con el derecho a la intimidad personal y familiar debido a la cercanía existente entre ambos derechos. En este sentido, resulta clarificadora la sentencia del Tribunal Constitucional de 30/11/2000, núm. 292/2000, en la cual se explica que la función del derecho fundamental a la intimidad es proteger de cualquier intromisión ilegítima el ámbito de la vida personal y familiar que cada persona desea excluir del conocimiento ajeno, mientras que el objeto del derecho fundamental a la protección de datos es garantizar a la persona *«un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»*. De lo anterior se concluye que el objeto de protección de este derecho fundamental abarca tanto los datos relacionados con la vida íntima de la persona como cualquier otro dato de carácter personal.

Adicionalmente, este derecho fundamental atribuye al titular de los datos personales el poder jurídico de imponer a terceros diferentes deberes jurídicos con el fin garantizar que ostenta un poder de control sobre sus datos personales, lo cual solo es posible mediante la imposición a terceros de determinados deberes de hacer. Estos deberes se refieren, por ejemplo, a la necesidad de recabar el consentimiento del titular de los datos personales con carácter previo a su recogida y uso, al deber de informar a este acerca del destino y uso que se va a dar a sus datos personales y el deber de posibilitar el ejercicio de distintos derechos como los de acceso, rectificación y cancelación. Además, el derecho a consentir el conocimiento y tratamiento de los datos personales por terceros, ya sean el Estado o un particular, requiere de la capacidad de conocer en todo momento quién dispone de los datos personales y en qué o para qué

'[…] Desde esta perspectiva, y en la medida en que la exigencia de resolución judicial a efectos de limitar un derecho fundamental posee carácter material, pues han de ser los Jueces y Tribunales los que autoricen el levantamiento del secreto de las comunicaciones ponderando la proporcionalidad de las medidas que afecten a este derecho fundamental y controlen su ejecución, hemos de considerar que, aunque desde luego la resolución judicial debe adoptar la forma de Auto, excepcionalmente también una providencia, integrada con la solicitud a la que se remite, puede cumplir las exigencias constitucionales en un caso como el analizado en el que se trata de autorizar el acceso a los listadostelefónicos por parte de la policía. Ello sucederá si la providencia, integradacon la solicitud policial a la que se remite, contiene todos los elementos necesarios para poder llevar a cabo con posterioridad la ponderación de la proporcionalidad de la limitación del derecho fundamental'».

finalidad los está empleando, así como tener la facultad de oponerse a esa posesión y usos.

Es indudable que los datos personales, como los datos biométricos, fiscales, sanitarios o de comunicaciones telefónicas, pueden ser fundamentales en la investigación de los hechos y en la prueba de los mismos ante cualquier orden jurisdiccional. De ahí la importancia de conocer las distintas habilitaciones legales existentes para la obtención de los datos personales sin conculcar el derecho fundamental a la protección de datos.

Una de ellas será el consentimiento del interesado (el titular de los datos personales) que, según dispone el artículo 6.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), deberá constituir una manifestación de voluntad específica, informada e inequívoca por la que se acepte el tratamiento de datos personales[44]. Más aun, tal y como específica el apartado segundo de dicho artículo, en caso de querer emplear los datos personales para una pluralidad de finalidades, el consentimiento deberá mostrarse específica e inequívocamente para todas ellas. No obstante, existen supuestos en los que no será necesario el consentimiento del interesado, como sucede, por ejemplo, cuando el tratamiento de los datos personales es necesario para el cumplimiento de una obligación prevista en una norma de Derecho de la Unión Europea o en una norma con rango de ley aplicable al responsable del tratamiento (artículo 8 LOPDGDD)[45]. Tampoco requerirá del consentimiento del interesado el tratamiento llevado a cabo por las Fuerzas y Cuerpos de Seguridad del Estado y los órganos judiciales para los fines de prevención, investigación, detección o enjuiciamiento de las infracciones penales o de ejecución de las sanciones penales. En este caso, se

[44] De acuerdo con lo dispuesto en el artículo 4.2) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante, RGPD), se entiende por tratamiento *«cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción»*.

[45] De igual modo, el artículo 6 RGPD prevé distintos supuestos en los que, al margen del consentimiento del interesado o del cumplimiento de una obligación legal, se entenderá lícito el tratamiento de los datos personales.

encuentran legalmente habilitados por la Ley Orgánica de Fuerzas y Cuerpos de Seguridad del Estado y por la Ley de Enjuiciamiento Criminal respectivamente[46].

A estos efectos, resulta ilustrativa la sentencia del Tribunal Superior de Justicia de Cataluña de 05/05/2011, núm. 11/2011, en la cual, al amparo del artículo 11 LOPJ, se declaró la nulidad de una grabación obtenida a partir de una cámara de videovigilancia que había sido aportada como prueba de cargo de una agresión. La escena de la agresión tuvo lugar fuera del campo de visión que debiera haber tenido aquella instalación de seguridad privada de cuerdo por la normativa vigente en aquel momento (la anterior LOPD), constatándose, de este modo, la vulneración del derecho fundamental del acusado a la protección de la imagen como datos personal. De hecho, en la medida en que el vigilante de seguridad no vio la agresión directamente sino que lo hizo a través de la cámara de videovigilancia, se anuló su testimonio conforme a lo razonado para la grabación de los hechos obtenida mediante dicho dispositivo de vigilancia que, como se ha dicho, no estaba correctamente instalado.

Dentro del ámbito laboral, la sentencia del Tribunal Constitucional de 11/02/2013, núm. 29/2013, determina que a pesar de que el tratamiento de datos resulte en principio lícito, por estar amparado por la ley (artículos 6.2 LOPD y 20 ET), y proporcional al fin perseguido atendiendo al caso concreto, no es posible llevar a cabo una limitación del derecho de información previa en la medida en que este integra la cobertura ordinaria del derecho fundamental a la protección de datos del artículo 18.4 CE. Por ello, en base a este razonamiento, el tribunal declaró la nulidad de la prueba derivada de las cámaras de videovigilancia que, captando la imagen del recurrente que constituye un dato de carácter personal, fueron empleadas para el seguimiento y control del cumplimiento de las obligaciones y deberes laborales sin haber informado

[46] En este sentido, se ha de advertir que, de acuerdo con lo dispuesto en la Disposición transitoria cuarta LOPDGDD, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) seguirá en vigor en relación a los tratamientos sometidos a la Directiva (UE) 2016/680, en tanto en cuanto no se apruebe la norma de transposición correspondiente. Así, el artículo 22.2 LOPD legitima la cesión de los datos obtenidos por particulares o por entidades públicas a las Fuerzas y Cuerpos de Seguridad para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, con el límite de los datos necesarios para la consecución de dichas finalidades; al tiempo que el artículo 11.2 d) LOPD y el artículo 236 quáter LOPJ hacen lo propio en relación al Ministerio Fiscal y los Jueces y Tribunales. Por su parte, el artículo 588 ter j.2 LECrim dispone que «*Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión*».

previamente al trabajador del posible empleo de las mismas como herramienta de supervisión laboral[47]. A dicha conclusión se llega sin perjuicio de que existieran distintivos que anunciaban la instalación de cámaras y la captación de imágenes en el recinto universitario y pese a haber notificado la creación del fichero a la Agencia Española de Protección de Datos.

1.2 Investigación y obtención de la prueba del hecho electrónico en el proceso civil

En sintonía con el carácter dispositivo del proceso civil, corresponde a las partes la investigación y obtención de la prueba relativa a los hechos electrónicos, que tendrá lugar, fundamentalmente, en el examen de la información o datos creados o almacenados en los dispositivos electrónicos, así como en el examen del contenido transmitido electrónicamente mediante redes de comunicación abiertas o restringidas.

En el examen de los dispositivos electrónicos, hay que distinguir los supuestos en que los datos se encuentran en un dispositivo de propiedad de la parte, de aquellos otros en que los datos se hallan en el dispositivo de un tercero o incluso de la parte contraria. En el primer caso, lo relevante será escoger adecuadamente el medio de prueba a través del cual se aportará la prueba del hecho electrónico al proceso, tratando de que, en la medida de lo posible, el mismo garantice su autenticidad e integridad; mientras que en el segundo caso, salvo que se acceda a la información contenida en dichos dispositivos por medio de orden judicial, el acceso a los datos que albergan estos dispositivos implicará la vulneración de derechos fundamentales.

En caso de que se pretenda acceder a los datos transmitidos a través de redes de comunicación, habrá que precisar, en primer lugar, si ha existido proceso de comunicación o si no, puesto que existen redes de comunicación como internet que permiten usos que no son encuadrables dentro de un proceso de comunicación (la navegación en la web, la actividad de una persona de agregar contenido a internet,…). Aclarado lo anterior, se deberá atender a las circunstancias del sujeto que accede al

[47] Igualmente, se ha entendido que la geolocalización o el historial de páginas web visitadas por el trabajador constituyen datos de carácter personales protegidos por el derecho a la protección de datos (sentencia del Tribunal Superior de Justicia de Madrid de 21/03/2014, núm. 260/2014 (Aranzadi) y sentencia del Tribunal Superior de Justicia de Andalucía de 28/03/2019, núm. 905/2019 (Aranzadi), respectivamente).

contenido de la comunicación, pues la afectación de unos u otros derechos fundamentales dependerá de que este haya sido o no parte del proceso de comunicación.

Con carácter general, dado que la LEC no prevé procedimientos que posibiliten a las partes el acceso a los datos contenidos en los dispositivos electrónicos de la parte contraria o de terceros, sucede que solamente tienen acceso a sus propios dispositivos electrónicos o a redes de comunicación como internet cuando no son de carácter restringido (redes sociales públicas, páginas web, etc.), lo que las lleva a aportar únicamente las pruebas que derivan de estos dispositivos o redes de comunicación. No obstante, el artículo 732.2 LEC, en sede de medidas cautelares, regula una excepción a esta limitación de la investigación forense que permite que el juez, a petición de parte, ordene las investigaciones que el solicitante no puede aportar o llevar a cabo por sí mismo en los casos en que se pretenda la prohibición o cesación de actividades ilícitas.

Asimismo, la LEC regula determinadas actuaciones preparatorias de la prueba que se examinaran a continuación, las cuales podrían servir, mediando un esfuerzo interpretativo, para la investigación de los dispositivos electrónicos del demandado, aunque por el momento no hay una jurisprudencia clara que abogue por el empleo de estas normas en el sentido indicado.

1.2.1 Diligencias preliminares

Las diligencias preliminares, en su carácter preparatorio del proceso, se encuentran íntimamente relacionadas con el derecho a la tutela judicial efectiva (artículo 24 CE), en la medida en que facilitan el ejercicio del derecho de acción. En concreto, al permitir la aclaración datos o la obtención de información que la parte solicitante no puede obtener por sí misma, se le ayuda a tener elementos suficientes para decidir sobre la procedencia de la interposición de la demanda o el alcance de las pretensiones a incluir en la misma. De este modo, en un intento por mantener la aplicabilidad de las diligencias preliminares en la realidad tecnológica y social actual, algunos autores han planteado que mediante una interpretación adaptada a la realidad social de los supuestos contemplados en el artículo 256 LEC, podría entenderse que en el término

"*documentos*" se extiende también a aquellos que se encuentran en soporte electrónico (un disco duro, un pendrive, un ordenador, un teléfono, etc.)[48].

Por lo demás, resulta destacable la inclusión, en los apartados 7, 8, 10 y 11 del artículo 256.1 LEC, de unas diligencias preliminares específicas para la obtención de datos en materia de propiedad intelectual o de propiedad industrial. Efectuando un conciso análisis de las medidas previstas en dichos apartados, cabe mencionar que se prevé la posibilidad de obtener los «*datos sobre el posible infractor, el origen y redes de distribución de las obras, mercancías o servicios que infringen un derecho de propiedad intelectual o de propiedad industrial*» (apartado 7), o «*la exhibición de los documentos bancarios, financieros, comerciales o aduaneros, producidos en un determinado tiempo y que se presuman en poder de quien sería demandado como responsable*» (apartado 8). En ambos casos, cuando las vulneraciones de estos derechos no se hayan producido por meros consumidores finales de buena fe y que no hayan obtenido beneficios económicos o comerciales, exigiéndose que la infracción de los derechos provenga de actos desarrollados a escala comercial, es decir, actos «*realizados para obtener beneficios económicos o comerciales directos o indirectos*». Seguidamente, el apartado 10 prevé la posibilidad de obtener los datos que permitan identificar a un prestador de un servicio de la sociedad de la información sobre el que haya indicios razonables de que está vulnerando derechos de propiedad intelectual o de propiedad industrial. Por último, el apartado 11 recoge la posibilidad de que el titular de un derecho de propiedad intelectual solicite al juez que un prestador de servicios de la sociedad de la información aporte los datos necesarios para la identificación de un usuario de sus servicios, cuando sobre este concurran indicios razonables de que está infringiendo derechos de propiedad intelectual, y no se trate de consumidores finales de buena fe y sin ánimo de obtención de beneficios económicos o comerciales.

Llegados a este punto, procede traer a colación lo dispuesto en el artículo 261 LEC, en relación a las posibles consecuencias de la negativa a llevar a cabo las diligencias preliminares acordadas por el juez civil. Entre ellas, se encuentra la posibilidad de acordar la entrada y registro del lugar en que se encuentran los títulos y

[48] Todo ello, en base a los criterios de interpretación de las normas que recoge el artículo 3.1 CC: «*Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas*».

documentos cuya exhibición se ha solicitado, cuando existan indicios suficientes para creer que se hallan en un concreto lugar. De igual modo, cabe que el juzgador tome por ciertas las cuentas y los datos presentados por el solicitante de la exhibición de documentos contables. En todo caso, ha de tenerse en cuenta que el tribunal acordará este tipo de medidas cuando resulte proporcionado y por medio de auto, lo cual descarta la aplicabilidad de estas medidas en cualquier situación ante cualquier tipo de resistencia o negativa a cumplir con las diligencias acordadas.

Para terminar con las diligencias preliminares, es preciso hacer referencia a lo dispuesto en el apartado noveno del artículo 256.1 LEC, el cual se remite a las diligencias y averiguaciones que eventualmente pudieran regular las correspondientes leyes especiales para la protección de determinados derechos. Ejemplo de ello son el artículo 123 de la Ley 24/2015, de 24 de julio, de Patentes, o el artículo 36 de la Ley 3/1991, de 10 de enero, de Competencia Desleal.

1.2.2 Deber de exhibición documental

De acuerdo con lo dispuesto en el artículo 328 LEC, cada una de las partes puede solicitar de las demás la exhibición de los documentos que no se encuentran a su disposición y que se refieren al objeto del proceso o a la eficacia de los medios de prueba. En concreto, para los procesos seguidos por infracción de un derecho de propiedad industrial o de un derecho de propiedad intelectual, el apartado tercero de dicho artículo prevé la extensión de este deber de exhibición a los documentos bancarios, financieros, comerciales o aduaneros producidos en un determinado periodo de tiempo y que se presume que se hallan en poder del demandado. En todo caso, la solicitud deberá ir acompañada de una copia simple del documento y, en caso de que esta no exista o no se disponga de ella, se deberá indicar de la forma más precisa posible cuál es su contenido.

Cuando la parte contraria cumpla con el deber de exhibición, los documentos aportados (la impresión de conversaciones de WhatsApp o de correos electrónicos, por ejemplo) surtirán los efectos que a nivel probatorio procedan. Por el contrario, si la parte adversa se niega a cumplir con el deber de exhibición, el artículo 329 LEC prevé los efectos que la negativa injustificada a la exhibición de los documentos puede acarrearle: el tribunal podrá, por un lado, atribuir valor probatorio a la copia simple presentada por

la parte que solicitó la exhibición o a la versión que haya ofrecido del contenido del documento cuando no pudiera aportar copia simple; o, por otro lado, formular requerimiento, mediante providencia, para que se aporten los documentos solicitados en caso de que así lo aconsejen las características de dichos documentos, las restantes pruebas aportadas, el contenido de las pretensiones formuladas por la parte solicitante y lo alegado para fundamentarlas.

Partiendo de un supuesto en el que el deber de exhibición se proyecte sobre los datos e informaciones almacenados en un ordenador, PINTO PALACIOS Y PUJOL CAPILLA entienden que lo adecuado sería requerir a la otra parte para que copie dicha información en algún dispositivo apto para su posterior lectura y examen. Con todo, admiten que esta opción puede plantear problemas al no quedar garantizada la integridad, fidelidad y exactitud de la información contenida en la copia aportada por la parte adversa. Por este motivo, al amparo de lo dispuesto en el artículo 336.5 LEC, proponen como posible solución la intervención de un perito informático que obtenga las copias con las debidas garantías[49]-[50].

De igual forma, la LEC regula la posibilidad de solicitar la exhibición de documentos a terceros (artículo 330), aunque en la práctica se emplea de forma excepcional, puesto que el tribunal, previa solicitud por una de las partes, solo requerirá la aportación a terceros de documentos de su propiedad cuando su conocimiento resulte trascendente para dictar sentencia. En caso de que el tribunal acceda, ordenará la comparecencia personal del tercero y, tras oírle, resolverá lo que proceda respecto de la aportación del documento al proceso. Cuando el tercero acceda a exhibir el documento voluntariamente, podrá solicitar que el Letrado de la Administración de Justica acuda a su domicilio para testimoniarlo, si bien en este caso el Letrado de la Administración de Justicia precisará de equipos informáticos con los que obtener copias de los archivos o

[49] Artículo 336.5 LEC: *«A instancia de parte, el juzgado o tribunal podrá acordar que se permita al demandado examinar por medio de abogado o perito las cosas y los lugares cuyo estado y circunstancias sean relevantes para su defensa o para la preparación de los informes periciales que pretenda presentar. Asimismo, cuando se trate de reclamaciones por daños personales, podrá instar al actor para que permita su examen por un facultativo, a fin de preparar un informe pericial».* En este caso, se entiende que los términos "*cosas y lugares*" que emplea el precepto incluyen también los datos contenidos en los dispositivos electrónicos de terceros, debiendo el juez emitir un juicio de ponderación de los derechos fundamentales afectados e intereses concurrentes, en caso de que el acceso de dichos dispositivos pudiera conculcar derechos fundamentales.

[50] PINTO PALACIOS, F. Y PUJOL CAPILLA, P. *La prueba en la era digital.* Wolters Kluwer, Madrid, 2017, págs. 141-142.

información relacionada con el hecho electrónico, pudiendo llegar a requerir la asistencia de un perito informático.

En caso de que el exhibiente no esté dispuesto a desprenderse del documento para su incorporación a los autos, el Letrado de la Administración de Justicia extenderá testimonio del mismo en la sede del tribunal, si así lo solicita el exhibiente. De modo similar, cuando se trate de dibujos, fotografías, croquis, planos, mapas y otros documentos que no sean textos escritos, y únicamente existiese el original, la parte puede solicitar que se obtenga copia del documento exhibido, garantizándose mediante la fe pública judicial del Letrado de la Administración de Justicia la exactitud e integridad de las copias. Además, debe señalarse que en caso de que los documentos hubieran sido aportados en forma electrónica, las copias que de aquellos realice la oficina judicial serán consideradas como copias auténticas.

Finalmente, el artículo 332 LEC recoge la obligación de las administraciones territoriales (Estado, Comunidades Autónomas, provincias y entidades locales), así como de las entidades de Derecho público, de exhibir los documentos que obren en sus dependencias y archivos, salvo en aquellos casos en que se trate de documentación legalmente declarada como reservada o secreta. No obstante, en este último caso la administración o entidad de Derecho público deberán dirigir al tribunal una exposición razonada sobre el carácter reservado o secreto del documento solicitado.

1.2.3 Medidas de aseguramiento de la prueba

Se trata de medidas que el juez puede adoptar a petición del demandante antes del inicio del proceso o durante el curso del mismo a petición de cualquiera de las partes, para evitar que, por conductas humanas o por acontecimientos naturales que puedan destruir o alterar objetos materiales o estados de cosas, resulte imposible practicar en su momento una prueba relevante o que pueda carecer de sentido incluso proponerla.

Estas medidas irán dirigidas a conservar las cosas o situaciones o hacer constar fehacientemente su realidad y características, o incluso podrán llegar a dirigirse mandatos de hacer o de no hacer, bajo apercibimiento de incurrir en un posible delito de desobediencia a la autoridad en caso de infringir dichos mandatos. Por otra parte, el

legislador introdujo, una vez más, medidas específicas para el caso de infracción de derechos de propiedad industrial y de propiedad intelectual (artículo 297.2.2º LEC).

1.2.4 Medidas cautelares

Como se ha venido explicando, la única norma que, sin necesidad de esfuerzos interpretativos, permite en el marco del proceso civil la investigación de los dispositivos electrónicos de la parte adversa se encuentra en el artículo 732.2 LEC, en sede de medidas cautelares, con el siguiente tenor: *«Cuando las medidas cautelares se soliciten en relación con procesos incoados por demandas en que se pretenda la prohibición o cesación de actividades ilícitas, también podrá proponerse al tribunal que, con carácter urgente y sin dar traslado del escrito de solicitud, requiera los informes u ordene las investigaciones que el solicitante no pueda aportar o llevar a cabo y que resulten necesarias para resolver sobre la solicitud».* De este modo, el tribunal podrá acordar *inaudita parte* que en el desarrollo de las investigaciones se obtengan los datos referidos al hecho electrónico que se hallen en los dispositivos electrónicos de la otra parte, con los que, en su caso, el solicitante fundamentará las pretensiones de la demanda[51].

En cualquier caso, de conformidad con lo dispuesto en el artículo 728.2 LEC, para la obtención de los elementos que prueben la existencia de una infracción por medio de esta medida cautelar, previamente el solicitante de las medidas cautelares debe aportar datos, argumentos y justificaciones documentales que ofrezcan un principio de prueba que funde su petición. A modo ejemplificativo, una empresa propietaria de determinados programas informáticos podría solicitar la autorización del juez para efectuar un registro de los dispositivos electrónicos de otra empresa, aportando elementos que le permitan al tribunal hacer un juicio provisional e indiciario favorable a la existencia de un uso fraudulento de dichos programas, pudiendo llegar a autorizarse la entrada y registro en la sede de la otra empresa[52].

[51] Pues en caso de no hallar elementos de prueba no se interpondrá de la demanda quedando a su vez sin efecto las medidas cautelares acordadas.

[52] El Juzgado de lo Mercantil nº8 de Barcelona, en su sentencia de 16/12/2019, núm. 291/2019, desestima la demanda de medidas cautelares en la que se solicitaba, al amparo del artículo 732.2 LEC la entrada y registro en el domicilio social de una empresa y la incautación y análisis de dispositivos informáticos de almacenamiento masivo de la información, por entender que se ha realizado una interpretación interesada de un mecanismo procesal que desborda su propio objeto y que afecta a derechos de otras partes. A lo que añade que *«para realizar en la jurisdicción penal una entrada y registro en el domicilio de una persona jurídica (art. 554 LECrim) el Juzgado de Instrucción debe extremar las cautelas y reforzar la*

Desde una perspectiva general, RICHARD GONZÁLEZ entiende que tanto por la naturaleza como por los efectos de esta medida cautelar, la misma debería hallarse regulada no en sede de medidas cautelares sino en sede de diligencias preliminares, como modalidad especial, con el efecto de obtener elementos de prueba que se encuentren en poder del demandado o futuro demandado. En este sentido, afirma que lo previsto en el artículo 732.2 LEC no puede considerarse como medida cautelar, al tiempo que cree incorrecta su limitación a aquellos supuestos de prohibición o cesación de actividades ilícitas, en tanto que podrían darse otros supuestos en los que fuera una medida útil y necesaria[53].

1.3 Investigación y obtención de la prueba del hecho electrónico en el proceso penal

Las medidas de investigación electrónica objeto de estudio fueron introducidas por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que supuso la positivización de las nuevas técnicas y necesidades de investigación existentes cuya implementación por la Policía Judicial resultaba indispensable, más aun en un momento en que la escueta regulación habida en este ámbito se encontraba indudablemente desactualizada con motivo del amplio desarrollo e implementación de las nuevas tecnologías[54]. De este modo, el Título VIII del Libro II de la LECrim recoge cinco capítulos dedicados a distintas medidas de investigación tecnológica limitativas de los derechos reconocidos en el artículo 18 CE, las cuales se concretan en la *«interceptación de las*

---

motivación de la correspondiente resolución judicial, siempre sobre la base de la existencia de suficientes indicios racionales de la comisión de un delito grave, parece que en un juicio mercantil, como el presente, que además ni siquiera ha comenzado, baste sin más una mera invocación de una denuncia anónima para acceder al domicilio de una persona jurídica que no ha cometido ningún ilícito penal y sin ningún tipo de oposición o contradicción procesal por aquélla […]Además, una vez ha sido desterrado de la jurisdicción penal el sistema inquisitivo, que se caracterizaba, entre otras cosas, por admitir la denuncia anónima, y se ha optado decididamente por un sistema acusatorio formal o mixto, propio de la Ilustración, en el que la denuncia debe identificar al denunciante (arts. 266 y 267 LECrim), la demandante pretende basar su pretensión civil en una suerte de denuncia anónima de muy dudosa legalidad».

[53] RICHARD GONZÁLEZ, M. "Investigación y prueba de hechos y dispositivos electrónicos", en *Revista General de Derecho Procesal*, 2017, pág. 28.

[54] En relación al adjetivo "tecnológico" otorgado por la Ley a las nuevas medidas de investigación, RICHARD GONZÁLEZ opina que, si bien es un término correcto, parecería más ajustado a la naturaleza, objeto y a las técnicas empleadas en su ejecución el vocablo "electrónicas", puesto que la tecnología también se halla presente en otras diligencias de investigación penal no adjetivadas como tecnológicas, en RICHARD GONZÁLEZ, M. "Investigación y prueba…", ob. cit. pág., 2017, pág. 16.

comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos»[55].

Como puede observarse, no todas las diligencias de investigación mencionadas afectan a los mismos derechos fundamentales, sino que dependiendo de la medida acordada el derecho fundamental afectado será uno u otro (derecho a la intimidad personal y familiar, al secreto de las comunicaciones y la libertad de circulación), o incluso varios al mismo tiempo. Por otra parte, cabe distinguir entre las medidas que implican la obtención directa o *in situ* de la prueba y aquellas otras que permiten la obtención remota de la misma, como ocurre en el caso de la interceptación de las comunicaciones, el control remoto de seguimiento y localización y los registros remotos de equipos informáticos.

Cabe destacar, igualmente, el marco normativo común aplicable a todas las medidas de investigación tecnológica contenido en los artículos 588 bis a – k LECrim, que abarca desde los principios rectores que han de presidir la autorización y ejecución de estas medidas, hasta el cese de la medida y la destrucción de los registros derivados de la ejecución de las mismas. En este sentido, la adopción de esta clase de diligencias de investigación requiere de autorización judicial habilitante que revestirá la forma de auto motivado (cuyo contenido mínimo viene predeterminado por el artículo 588 bis c.3 LECrim), el cual habrá de respetar los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida, que vienen definidos por el propio artículo 588 bis a LECrim[56].

[55] La Fiscalía General del Estado publicó cinco circulares en las que se incluyen una serie de pautas de interpretación de estas medidas, las mencionadas circulares son las siguientes: Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal; Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas; Circular 3/2019, de 6 de marzo, de la Fiscal General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; y Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.

[56] De esta forma, el principio de especialidad requiere que la resolución judicial que acuerde la práctica de una de estas diligencias indique el delito concreto que se investiga e identifique a los sujetos sospechosos

En todo caso, hay que tener en cuenta que la norma limita la capacidad de solicitar al juez de instrucción las medidas de investigación tecnológica al Ministerio Fiscal y a la Policía Judicial, pudiendo, en su caso, ser acordadas de oficio por el propio juez. En cualquier caso, ello no es óbice, tal y como se afirma en la Circular 1/2019, para que la acusación particular o popular puedan proponer al juez alguna de estas medidas. En estos casos, cuando el juez asuma la propuesta de la acusación y proceda a acordarla de oficio, procederá de conformidad con lo dispuesto en el artículo 588 bis d LECrim y una vez acordada alguna de estas medidas decretará una pieza separa y secreta para su desarrollo, la cual será notificada a la parte que la propuso en el momento en que se alce el secreto de la pieza separada[57].

La medida que eventualmente pueda acordarse tendrá la duración que se determine en el auto que la autorice sin que pueda exceder del tiempo imprescindible para el esclarecimiento de los hechos, o de lo establecido en el auto que la prorrogue de oficio o a petición razonada del solicitante cuando se mantengan las causas que la motivaron. Así pues, el juez acordará el cese de la medida en el momento en que desaparezcan las circunstancias que motivaron su adopción, o cuando haya certeza de que la medida no está logrando los resultados esperados y, por supuesto, cuando haya transcurrido el plazo por el que fue autorizada.

---

investigados. En concordancia con lo anterior, las investigaciones prospectivas o genéricas, o aquellas que tengan por objeto prevenir o descubrir delitos o aclarar sospechas carentes de base objetiva, quedan excluidas del ámbito de aplicación de estas medidas.

Por otro lado, la idoneidad de la medida de investigación tecnológica sirve para determinar los ámbitos objetivo (que la medida sea lo menos invasiva posible de los derechos fundamentales), subjetivo (que afecte el menor número posible de personas) y la duración (mínima necesaria y siempre dentro de los plazos previstos en la ley) de la medida de acuerdo con su utilidad.

Por su parte, los principios de excepcionalidad y necesidad implican la necesidad de que, o bien los investigadores no dispongan de otras medidas alternativas útiles para el esclarecimiento de los hechos y menos gravosas para los derechos fundamentales del investigado o encausado, o bien que el no recurrir a estas medidas suponga dificultar gravemente el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito.

Finalmente, la debida observancia del principio de proporcionalidad exige, atendiendo a las circunstancias del caso concreto, tener en cuenta los bienes o valores concurrentes y la ponderación de los intereses en juego, para así poder determinar cuando el sacrificio de los derechos e intereses individuales comporta un mayor beneficio para el interés público y de terceros. A estos efectos, el apartado 5 del artículo 588 bis a LECrim fija los criterios en los que se basa la ponderación del interés público.

[57] De acuerdo con la conclusión decimocuarta de la Circular 1/2019: «*Cada medida de investigación tecnológica que se tramite dará lugar a la formación de una pieza separada y secreta distinta, sin que resulte correcta la tramitación de varias de ellas en una misma pieza. Ello, no obstante, deberá incluirse en la misma pieza todo lo concerniente a la ejecución de cada medida de investigación tecnológica que afecte al mismo investigado, aunque recaiga sobre diversos dispositivos*».

En cuanto al control de la medida por el juez de instrucción, la Policía Judicial le informará del desarrollo y de los resultados de la medida, en la forma y con la periodicidad que este determine y siempre que por cualquier causa se ponga fin a la misma.

Dicho esto, en los apartados que siguen se efectuará un estudio más pormenorizado de las diligencias de investigación tecnológica referidas a la interceptación de las comunicaciones telefónicas y telemáticas (artículos 588 ter a – m LECrim), los registros de dispositivos de almacenamiento masivo de información (artículos 588 sexies a – c LECrim) y los registros remotos sobre equipos informáticos (artículo 588 septies a – c LECrim)[58].

1.3.1 Interceptación de las comunicaciones telefónicas y telemáticas

La autorización judicial que habilite la interceptación de las comunicaciones telefónicas y telemáticas se concederá para la investigación de: delitos dolosos castigados con pena cuyo límite máximo sea de, al menos, tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal o en el caso de delitos de terrorismo, así como en relación a los delitos cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. Dentro de los elementos que se tienen en consideración a la hora de realizar la ponderación de los intereses en conflicto, al objeto de determinar la proporcionalidad o no de esta medida que afecta al secreto de las comunicaciones, este se refiere a la gravedad del hecho. La concurrencia del mismo no es suficiente para superar el juicio de proporcionalidad sin tener en cuenta la trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido.

La solicitud de autorización judicial para la interceptación de las comunicaciones telefónicas o telemáticas deberá cumplir no solo con los requisitos recogidos en el artículo 588 bis b LECrim, sino también con los requisitos específicos

[58] Para conocer más sobre la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos o sobre la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen véase DÍAZ MARTÍNEZ, M. Y LÓPEZ-BARAJAS PEREA, I. *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas.* Tirant Lo Blanch, Valencia, 2018.

establecidos al efecto por el artículo 588 ter d.1 LECrim. De este modo, deberá contener la identificación del número de abonado, del terminal o de la etiqueta técnica; la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate. Por otro lado, el artículo 588 ter d.2 LECrim delimita el alcance de la medida al registro y grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta; al conocimiento de su origen o destino, en el momento en el que la comunicación se realiza; a la localización geográfica del origen o destino de la comunicación, y al conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

No obstante, por motivos de urgencia y por concurrir elementos que hagan imprescindible la adopción de esta medida, en el marco de las investigaciones de los delitos relacionados con la actuación de bandas armadas o elementos terroristas, cabe la posibilidad de que esta sea ordenada por el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Ahora bien, en este caso habrá que comunicar la adopción de la medida al juez competente lo antes posible y, como máximo, dentro de las 24 horas siguientes a la adopción de la misma, debiendo exponer las razones que justificaron la adopción de la medida sin previo control judicial, la actuación realizada, la forma en que se ha llevado a cabo y el resultado obtenido. En base a lo anterior, el juez revocará o confirmará dicha actuación en un plazo máximo de setenta y dos horas desde que la medida fue ordenada.

De cualquier manera, esta medida afectará a los terminales o medios de comunicación habitual u ocasionalmente empleados por el investigado, ya sea como emisor o receptor, de los que sea titular o usuario, y permitirá acceder al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a aquellos que se producen haya o no una concreta comunicación. Asimismo, los terminales o medios de comunicación telemática de terceras personas pueden verse afectados por esta medida cuando se constate su empleo por el investigado para transmitir o recibir información, o en caso de que el titular colabore con el investigado en sus fines ilícitos o se esté beneficiando de su actividad. Cabe destacar, además, la posibilidad de intervenir los terminales o medios de

comunicación de la víctima cuando sea probable que se produzca un grave riesgo para su vida o integridad.

Cuando los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación sean imprescindibles para el buen curso de la investigación, se solicitará al juez competente que autorice la recogida de la información que conste en los archivos automatizados de los prestadores de servicios, incluidos los datos derivados de la búsqueda entrecruzada o inteligente de los mismos, siempre y cuando se concrete la naturaleza de los datos que deban conocerse y los motivos que justifican la cesión (artículo 588 ter j LECrim).

Seguidamente, la LECrim regula la forma en que la Policía Judicial tendrá acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad. De un lado, el artículo 588 ter k LECrim se refiere a la identificación de dichos extremos por medio de una dirección IP. En este caso, en el marco del ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, la Policía Judicial solicitará al juez de instrucción que requiera a los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

De otro lado, el artículo 588 ter l LECrim faculta a la Policía Judicial para que en el marco de una investigación emplee las técnicas que permitan conocer los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de sus componentes, tales como la numeración IMSI o IMEI. Adicionalmente, y, con carácter general, la Policía Judicial podrá valerse de cualquier medio técnico que sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones (todo ello sin necesidad de autorización judicial)[59]. Una vez

[59] Sobre el IMSI O IMEI ARRABAL PLATERO explica que «*El IMSI –acrónimo de International Mobile Suscriber Identity- es un código de identificación único para cada dispositivo móvil, integrado en la tarjeta chip SIM que se inserta en el teléfono móvil para asignarle el número de abonado o MSISDN –Mobile Station Integrated Services Digital Network-, que permite su identificación a través de redes GSM. Este número de abonado está compuesto por el MCC o código del País (tres dígitos), por ejemplo, 214, que correspondería a España; por el MNC o Código de la red móvil (dos o tres dígitos), por ejemplo 07, que correspondería a la operadora MOVISTAR; y finalmente por el MSIN (número de diez dígitos) que contiene la identificación de la estación móvil. Es posible obtener el número IMSI de un teléfono móvil mediante un dispositivo que debe aproximarse al teléfono que se desea investigar y que simula el comportamiento de la red GSM, de forma tal que interactúa de manera equivalente a cómo lo hace una infraestructura de red de un operador móvil con un teléfono móvil que se enciende o que*

conocidos los códigos de identificación del aparato o de alguno de sus componentes, la Policía Judicial podrá solicitar del juez competente la intervención de las comunicaciones, incluyendo en su solicitud una explicación de los artificios utilizados para conocer dichos códigos de identificación.

Finalmente, en cuanto a la identificación de usuarios, terminales y dispositivos de conectividad, el artículo 588 ter m LECrim dispone que el Ministerio Fiscal o la Policía Judicial puedan dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información (quienes se encuentra obligados a colaborar bajo apercibimiento de incurrir en un delito de desobediencia), cuando, en el ejercicio de sus funciones, precisen conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o conociendo esta, para tener conocimiento del número de teléfono o los datos identificativos de cualquier medio de comunicación.

Por su parte, los sujetos obligados en virtud del artículo 588 ter e LECrim a prestar la asistencia y colaboración necesarias para el cumplimiento de los autos que acuerden la intervención de las comunicaciones, deberán guardar secreto acerca de las actividades requeridas, pudiendo incurrir, como se ha dicho anteriormente, en un delito de desobediencia en caso de incumplimiento del deber de colaboración. Dicho deber legal deberá acatarse durante toda la duración de la medida, cuyo *dies a quo* será la fecha de la autorización judicial, la cual inicialmente acordará la intervención por un plazo de 3 meses prorrogables en períodos sucesivos de igual duración hasta alcanzar el plazo máximo de 18 meses.

En lo que respecta a las partes, estas tendrán acceso a la copia de las grabaciones y de las transcripciones realizadas una vez se alce el secreto y expire la vigencia de la medida de investigación. Además, las partes estan facultadas para solicitar al juez de instrucción la inclusión en las copias de las comunicaciones de los fragmentos que entiendan relevantes y que hayan sido excluidas. Al mismo tiempo, el artículo 588 ter i LECrim prevé la eliminación de los aspectos de la vida íntima de las personas, así como la posibilidad de notificar a las personas intervinientes en las comunicaciones intervenidas la práctica de esta medida e informarles de cuales han sido las

cambia de célula de cobertura», en ARRABAL PLATERO, P. *La prueba tecnológica…*, ob. cit., 2020, págs. 222-223.

comunicaciones afectadas, salvo cuando sea imposible, exija un esfuerzo desproporcionado o pueda perjudicar futuras investigaciones.

1.3.2 Registro de dispositivos de almacenamiento masivo de información

En virtud de esta medida de investigación, el juez podrá autorizar la aprehensión de distintos dispositivos aptos para el almacenamiento masivo de la información (ordenadores, teléfonos móviles, discos duros, USBs, pen drives, *tablets*, tarjetas de memoria, etc.), el examen de su contenido y la realización de copias de la información contenida en ellos relacionada con el delito investigado en el proceso penal. Se trata, por tanto, de una medida que afecta tanto al derecho a la intimidad como al secreto de las comunicaciones. Si bien es cierto que se evitará la aprehensión de estos dispositivos cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible obtener una copia de los datos o archivos informáticos en condiciones en que se garantice la autenticidad e integridad de los mismos, salvo que estos soportes constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen.

Nótese que, a estos efectos, el artículo 588 sexies a LECrim requiere de una autorización judicial especial para la realización de dicho examen (también posible cuando medie consentimiento del titular de la vivienda o en caso de delito flagrante), de tal suerte que la práctica de un registro domiciliario no legitima *per se* a acceder a la información contenida en los dispositivos de almacenamiento masivo de la información incautados[60]-[61]. Por este motivo, cuando sea probable el descubrimiento de dichos dispositivos y se reputa necesario el examen de los mismos, lo habitual es incluir en la misma resolución judicial la autorización relativa al registro domiciliario y la referida al acceso a la información comprendida en dichos dispositivos, con motivación individualizada. En este sentido, la resolución judicial que habilite a examinar el contenido de los dispositivos de almacenamiento masivo de la información deberá

[60] De conformidad con lo establecido en la Circular 5/2019, el consentimiento puede manifestarse expresa o tácitamente, en este último caso, debe tratarse no de expresiones sino de actos concluyentes que exterioricen una inequívoca voluntad de colaborar con el registro, sin que pueda admitirse como un consentimiento tácito la simple falta de oposición al mismo. En suma, el consentimiento, sea expreso o tácito, ha de ser inequívoco y libre (sin vicios del consentimiento del artículo 1265 CC).

[61] Además, extiende dicho requisito a aquellos supuestos en que se lleve a cabo la incautación de estos dispositivos fuera del marco de un registro domiciliario. Por otra parte, cabe destacar que a diferencia de lo que ocurre en la interceptación de las comunicaciones telefónicas y telemáticas, en este caso la LECrim no exige que la investigación tenga por objeto una concreta clase de delitos.

expresar los términos y el alcance del registro y podrá autorizar la realización de copias, al tiempo que determinará las condiciones y garantías que aseguren la integridad y preservación de los datos en vistas a la eventual práctica de un dictamen pericial.

No obstante lo anterior, existen circunstancias en las que la Policía Judicial puede proceder al examen de los datos contenidos en un dispositivo sin autorización judicial previa. Así se prevé en los apartados 3 y 4 del artículo 588 sexies c LECrim que, al amparo de situaciones de urgencia, permiten la ampliación del registro a otros sistemas informáticos o a parte de los mismos cuando haya razones fundadas para pensar que los datos buscados se hallan en los mismos, o la adopción de esta medida cuando se aprecie un interés constitucional legítimo que la haga imprescindible (en este supuesto, además, careciendo de orden judicial previa). En ambos casos, se informará inmediatamente al juez (en el plazo máximo de veinticuatro horas) de la actuación realizada, la forma en que se ha efectuado y el resultado obtenido; en base a lo cual el juez revocará o confirmará esta actuación en un plazo máximo de setenta y dos horas desde que la medida fue ordenada.

Con respecto a esta posibilidad, distintos autores han advertido del peligro de que en la práctica suponga una reducción del control judicial, dado que se cree difícil garantizar que las intromisiones que se produzcan en los derechos fundamentales del investigado, con base a motivos de urgencia, vayan a ser comunicadas sin excepción al órgano judicial, sobre todo en relación a aquellas medidas que hayan resultado infructuosas por no encontrar los instrumentos o efectos del delito. En estos casos, en los que la medida no ha tenido los resultados esperados, los agentes de la Policía Judicial únicamente aspirarían a la confirmación de una medida que no contribuye a su investigación, lo cual desincentiva la práctica esta comunicación al ser fácilmente percibida como innecesaria o una pérdida de tiempo.

Asimismo, es importante subrayar la existencia de un específico deber de colaboración recogido en el artículo 588 sexies c.5 LECrim, en virtud del cual las autoridades y agentes encargados de la investigación pueden ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para la protección de los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, eximiéndose a quienes dicho deber les suponga una carga desproporcionada, quedando el resto obligados bajo apercibimiento de incurrir en

un delito de desobediencia en caso de incumplimiento. Ahora bien, esta obligación tampoco afectará al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de acuerdo con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional.

1.3.3 Registros remotos sobre equipos informáticos

La diligencia de investigación objeto del presente apartado guarda ciertas similitudes con el registro de dispositivos de almacenamiento masivo de la información en la medida en que ambas se proyectan sobre los mismos dispositivos (ordenadores, teléfonos móviles, discos duros, USBs, pen drives, *tablets*, tarjetas de memoria, etc.), y que comparten la misma finalidad, que no es otra que la búsqueda y descubrimiento de pruebas o indicios del delito en los datos o informaciones electrónicas de los dispositivos. Sin embargo, ambas diligencias de investigación difieren en importantes aspectos, como lo son el conocimiento de la sustanciación de la medida por parte del investigado titular o usuario del dispositivo, el carácter estático o dinámico del registro y la exigencia de que la investigación tenga por objeto determinados delitos.

De esta forma, tal y como expresamente prevé el artículo 588 septies a LECrim, el registro remoto sobre equipos informáticos se lleva a cabo sin el conocimiento del afectado, al tiempo que la adopción de esta medida se supedita, entre otras cosas, a la investigación de determinados delitos[62]. Por otro lado, merece una mención especial el carácter dinámico del registro remoto, el cual determina una capacidad de intromisión y una intensidad de dicha intromisión mucho mayor que la que implica el registro directo del contenido estático del dispositivo o sistema. Ello es así en tanto que el registro dinámico incrementa notablemente la cantidad de datos a los que se tiene acceso ya que no solo permite el registro del contenido de un dispositivo en un determinado momento, sino que igualmente posibilita conocer lo que se va agregando y/o eliminando del

[62] Artículo 588 septies a.1 LECrim: *«…siempre que persiga la investigación de alguno de los siguientes delitos: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*». En lo concerniente a la inclusión de los delitos a que hace referencia la letra e) de este artículo, la doctrina ha criticado la equiparación, sin más especificación, del hecho delictivo cometido por medio de las nuevas tecnologías con otros delitos tan graves como los de terrorismo, en tanto en cuanto los delitos cometidos valiéndose de estos instrumentos pueden ser de escasa importancia, sin que en estos casos parezca razonable ni apropiada la utilización de esta medida.

mismo durante la vigencia de la medida. Evidentemente, la principal consecuencia de lo anterior es el mayor grado de injerencia en los derechos fundamentales a la intimidad y al secreto de las comunicaciones[63]; sin olvidar que, de acuerdo con la Circular 5/2019, también se afectará al derecho fundamental de creación jurisprudencial relativo al derecho al entorno virtual[64]. Este último derecho abarca la protección de la amplia heterogeneidad de datos que pueden almacenarse en un dispositivo o sistema informático, los cuales individualmente considerados serían susceptibles de afectar a diferentes derechos fundamentales como los anteriormente señalados.

Es precisamente esta mayor injerencia en los derechos fundamentales del investigado lo que justifica el establecimiento de mayores limitaciones en la regulación de esta medida. En tal sentido, puede señalarse el requisito ya mencionado de que la investigación se circunscriba a una clase determinada de delitos, o el hecho de que, a diferencia de lo que sucede en la diligencia de investigación recogida en el apartado anterior, no cabe realizar un registro policial previo a la autorización judicial pues se considera que no existe dicha situación de urgencia cuando el investigado desconoce el desarrollo de esta diligencia.

De este modo, la adopción de esta medida queda condicionada a la previa autorización judicial mediante auto motivado que permita el acceso y examen a distancia del contenido de un dispositivo electrónico o sistema informático que, con carácter general, requerirá que dichos equipos se encuentren en funcionamiento o, al menos, en línea, para ser efectiva[65]. En todo caso, el auto que acuerde el registro deberá cumplir, en cuanto a su contenido, con lo previsto en los artículos 588 bis.3 y 588

[63] Este aspecto queda claramente explicado en la Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos: *«El carácter estático del registro propio de los registros directos podrá determinar que resulten afectadas conversaciones puntuales cuyo proceso de comunicación no haya concluido, como podrían ser los correos electrónicos no leídos, mientras que, en los registros remotos, su carácter dinámico posibilita la interceptación de comunicaciones a tiempo real y su seguimiento durante todo el tiempo que dura la medida».* Sin olvidar el hecho de que hay autores que plantean una posible intromisión en el derecho a la inviolabilidad del domicilio cuando se trate de un ordenador fijo instalado en la vivienda.

[64] La sentencia del Tribunal Supremo de 10/03/2016, núm. 204/2016 (Aranzadi), alude de la siguiente forma al derecho a la protección del propio entorno virtual también conocido como derecho a la privacidad del entorno virtual o digital: *«Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos».*

[65] RICHARD GONZÁLEZ, M. "Investigación y prueba…", ob. cit., 2017, pág. 20.

septies a.2 LECrim. El acceso a los dispositivos electrónicos o sistemas informáticos que procedan se llevará a cabo por medio de datos de identificación y códigos, mediante la instalación de un software (conocido como "troyano" o *spyware*), o a través de la instalación de un *keylogger*, que es un software o hardware capaz de interceptar y guardar las pulsaciones que se realizan en el teclado de un equipo que haya sido infectado.

La duración máxima de esta medida será de un mes prorrogable por iguales periodos hasta un máximo de tres meses, si bien es cierto que no es preciso agotar los plazos por los que se haya sido autorizada en tanto que persiste la obligación de mantener la medida solo por el tiempo estrictamente necesario para el esclarecimiento de los hechos. Según entiende BACHMAIER WINTER, lo adecuado sería tomar como *dies a quo* el momento en que el equipo resulta accesible al estar el *software* instalado y operativo, mientras que el *dies ad quem* debería corresponderse con el momento en que se finalice la clonación del contenido del dispositivo electrónico o sistema informático[66].

Finalmente, cabe destacar que una vez más la LECrim prevé un deber de colaboración que recae sobre los prestadores de servicios y personas señaladas en el artículo 588 ter e LECrim, así como sobre los titulares o responsables del sistema informático o base de datos objeto del registro. Estos últimos deberán colaborar en la medida en que resulte necesario con los agentes investigadores para que estos puedan practicar la medida, acceder al sistema y tener la asistencia necesaria para que los datos y la información recogidos puedan ser examinados y visualizados. Por otro lado, las autoridades y agentes encargados de la investigación pueden ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para la protección de los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria. No obstante, esta obligación tampoco afectará al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de acuerdo con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional. El resto de individuos quedan obligados a guardar secreto respecto de las actividades requeridas en el marco

[66] BACHMAIER WINTER, L. "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", en *Boletín del Ministerio de Justicia*, nº2195, 2017, pág. 18.

de la diligencia de investigación, con la advertencia de poder incurrir en un delito de desobediencia en caso de incumplimiento de los anteriores deberes.

1.4 Investigación y obtención de la prueba del hecho electrónico en el proceso laboral

La progresiva e imparable introducción de las nuevas tecnologías en el ámbito laboral ha afectado no solo al modo en que trabajamos, sino también a la forma en que se manifiestan las situaciones conflictivas propias de este ámbito. En este sentido, la investigación sobre los dispositivos o medios electrónicos que la empresa pone a disposición de los trabajadores como instrumentos para la prestación de sus servicios, se ha convertido en uno de los ámbitos en que mayor desarrollo jurisprudencial ha tenido la investigación de los hechos electrónicos. Así, sobre la base del poder de vigilancia y control otorgado al empresario en virtud del artículo 20.3 ET, la jurisprudencia ha venido estableciendo diferentes pautas con relación a la forma en que ha de producirse la investigación forense de los dispositivos electrónicos, siempre procurando el debido respeto de los derechos fundamentales al secreto de las comunicaciones y a la intimidad, cuya afectación pudiera derivar en la ilicitud de las pruebas obtenidas en el proceso de investigación[67]. En cualquier caso, lo cierto es que no es posible establecer reglas absolutas aplicables a la totalidad de las situaciones, dada la amplitud de variables y circunstancias que pueden darse en cada caso concreto.

Sin embargo, uno de los puntos más claros lo constituye la necesidad de que el trabajador sea previamente informado acerca de las normas de uso de los dispositivos electrónicos puesto a su disposición (que normalmente consisten en limitar su uso para fines laborales o profesionales con prohibición expresa de otro tipo de usos), así como de la vigilancia y control que a este respecto puede llevar a cabo la empresa, especificando el alcance de dicho control y las eventuales consecuencias que pudieran

[67] En esta línea, cabe mencionar lo dispuesto en el artículo 87 LOPDGDD, que se refiere al derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral, reafirmando el preceptivo respeto de la intimidad de los trabajadores, al tiempo que reconoce la facultad del empresario de controlar el uso de los medios digitales como forma de controlar el cumplimiento de las obligaciones laborales y que prevé la necesidad de establecer criterios de utilización de estos dispositivos. De igual modo, cabe destacar que el apartado tercero de este precepto prevé la posibilidad de que la empresa autorice el uso para fines privados, en cuyo caso será necesaria una información mucho más detallada acerca de los usos privados permitidos, cuándo se permiten, las garantías de privacidad, etc. (a este respecto la sentencia del Tribunal Europeo de Derechos Humanos de 22/02/2018, Caso Libert contra Francia).

derivarse del incumplimiento de las normas de uso[68]. En estos casos, no existirá expectativa razonable de intimidad o privacidad quedando legitimada la actuación empresarial de control. A *sensu contrario,* cuando la empresa no advierta a los trabajadores de la posibilidad de que su actividad sea fiscalizada, la intervención y control empresarial implicará la vulneración de los derechos al secreto de las comunicaciones y a la intimidad (artículos 18.1 y 3 CE y 8 CEDH), tal y como se declara en la sentencia del Tribunal Europeo de Derechos Humanos de 03/04/2007, Caso Copland contra Reino Unido, en un caso en que a la trabajadora no se le advirtió de que sus llamadas podían ser objeto de seguimiento.

De este modo, sobre la base de la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos (Casos Copland contra Reino Unido y Barbulescu contra Rumania), del Tribunal Constitucional y del Tribunal Supremo, especialmente en relación a la sentencia del Tribunal Supremo de 08/02/2018, núm. 119/2018, RICHARD GONZÁLEZ realiza una concisa enumeración de los principios sobre los que se sustenta la doctrina jurisprudencial relativa al control empresarial de los medios de comunicación de la empresa puestos a disposición del trabajador, destacándose los siguientes[69]:

- El derecho fundamental a la intimidad (y al secreto de las comunicaciones) se extiende a la información contenida en los discos duros o tarjetas de memoria

[68] Así lo expresa la sentencia del Tribunal Supremo de 26/09/2007, núm. rec. 966/2006 (Aranzadi): *«Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos».*

[69] RICHARD GONZÁLEZ, M. "Reglas para la investigación forense y aportación como prueba al proceso de correos y mensajes electrónicos del trabajador (comentario a la STS sala cuarta de lo social, nº119/2018 de 8 feb. 2018, rec.1121/2015. LA LEY 4068/2018)", en *Diario LA LEY*, 2018. Asimismo, véase el análisis conjunto de la sentencia del Tribunal Supremo de 08/02/2018, núm. 119/2018, y su adecuación a la doctrina del Tribunal Europeo de Derechos Humanos (Caso Barbulescu) efectuada en MONREAL BRINGSVAERD, E., THIBAULT ARANDA, X. Y JURADO SEGOVIA, A. *Derecho del trabajo y nuevas tecnologías. Estudios en homenaje al profesor Francisco Pérez de los Cobos Orihuel*, Tirant lo Blanch, Valencia, 2020, págs. 214-223.

contenidas en los ordenadores o teléfonos, tanto personales como de la empresa[70].

- La implementación en la empresa de una normativa que regule la utilización de los dispositivos (en cuya elaboración deben participar los representantes de los trabajadores), de forma que los trabajadores conozcan previa y claramente qué usos son lícitos y cuales están taxativamente prohibidos, así como los procedimientos que pueden emplearse para su control, elimina toda expectativa razonable de privacidad o confidencialidad del trabajador[71]. A título ilustrativo, cabe mencionar el caso resuelto por la sentencia del Tribunal Supremo de 08/02/2018, núm. 119/2018, en el que la empresa no solo tenía una concreta regulación referida a la Política de Seguridad de la Información y del uso de los sistemas de información, sino que cada vez que se accedía al ordenador se mostraba un aviso recordando que dicho medio y los programas instalados en él eran de propiedad de la empresa y para fines exclusivamente laborales; con advertencia de la vigilancia y control practicada por la empresa y requiriendo la conformidad del empleado con dichos términos. Así, todos los trabajadores conocían perfectamente los fines para los que se habilitaba el acceso y uso a los ordenadores y las posibles medidas de vigilancia y control empresarial.
- El empresario podrá establecer las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación el respeto debido a los derechos fundamentales, la consideración debida a la dignidad humana y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad[72].

---

[70] En este mismo sentido lo entiende el Tribunal Constitucional en su sentencia de 07/11/2011, núm. 173/2011, al señalar que *«el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email , escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado»*.

[71] Y en estos casos, como señala la sentencia del Tribunal Supremo de 06/10/2011, núm. rec. 4053/2010 (Aranzadi): *«al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo»*. Con todo, aun en el caso de prohibición expresa, sigue siendo exigible el respeto de unos estándares mínimos de intimidad y secreto de las comunicaciones.

[72] En cualquier caso, la calificación como ilícita de alguna de las pruebas en las que se funda el despido no conlleva la nulidad del mismo, sino solamente la de dicha prueba, pudiendo el despido llegar a ser declarado improcedente por falta de justificación pero no nulo (sentencia del Tribunal Constitucional de 15/03/2021, núm. rec. 6838/2019, Aranzadi).

- Las medidas de control empresarial alcanzan también a los medios tecnológicos de comunicación puestos a disposición del trabajador, incluidas las cuentas de correo electrónico corporativo otorgadas a los trabajadores. Las cuentas de correo electrónico particulares, por su parte, no pueden ser objeto de control empresarial aunque sí que puede prohibirse su instalación y uso. De modo que la investigación forense no debe ir más allá de la constatación del incumplimiento de las normas de uso (instalación de aplicaciones personales, uso del correo electrónico personal, etc.), y, de ser necesario acceder a esta información, se deberá proceder en vía penal contra el trabajador solicitando la autorización judicial correspondiente.
- El poder de control empresarial, legítimamente ejercido de acuerdo con lo establecido en los puntos anteriores, comprende tanto la comprobación del cumplimiento de las obligaciones y deberes laborales, como la vigilancia de los fines propios o ajenos a la prestación laboral a los que se destinan los dispositivos electrónicos facilitados por la empresa. A mayor abundamiento, hay que tener en cuenta que el uso indebido de los medios de la empresa constituye infracción grave en muchas normas convencionales. Los anteriores fines de la vigilancia y control, junto con el de garantizar la integridad de los dispositivos al que hace referencia el artículo 87.2 LOPDGDD, constituyen la justificación legítima a la que alude la sentencia del Tribunal Europeo de Derechos Humanos de 05/09/2017, Caso Barbulescu contra Rumania.
- La medida de investigación empleada en el análisis forense de los dispositivos debe ser idónea, necesaria y equilibrada o proporcional[73]. De esta forma, el examen de la información contenida en los archivos y/o registros de los dispositivos de la empresa no puede efectuarse de forma indiscriminada, exhaustiva o ilimitada.
- En relación con lo anterior, la investigación forense debe efectuarse utilizando herramientas informáticas que permitan el análisis selectivo de los archivos, mensajes y correos. A estos efectos, la técnica más conocida se identifica con el empleo de palabras clave relacionadas con el objeto de la investigación, tratando

[73] La medida será idónea cuando sea susceptible de conseguir aquello que se propone, será necesaria en caso de que no exista otra medida menos lesiva e igual de eficaz para la consecución del objetivo, y será proporcional cuando de ella resulten más beneficios o ventajas para el interés general que perjuicios sobre los distintos bienes o valores en conflicto.

así de no alcanzar a los datos de naturaleza privada amparados por el derecho a la intimidad.

- El acceso y posterior análisis de los archivos y/o registros contenidos en los dispositivos electrónicos y en los programas o sistemas de comunicación o información corporativos, no supondrá la vulneración de los derechos fundamentales del trabajador. Con todo, ello no habilita al perito forense a efectuar una investigación que abarque todos los mensajes y datos habidos en el dispositivo o servidor de la empresa, puesto que siempre han de quedar al margen de la investigación los datos o correos con contenido personal del trabajador que no guarden relación con la actividad. Todo ello, sin perjuicio de que la constatación de usos no autorizados o de la instalación de aplicaciones personales pueda constituir causa suficiente para motivar el despido del trabajador u otra sanción.
- Ahora bien, en el caso de los dispositivos de uso común a todos los trabajadores sin ninguna contraseña u obstáculo para acceder a los mismos (como, por ejemplo, encontrarse en un despacho cerrado con llave), la empresa, previa información de las normas de uso y de su capacidad de control, puede verificar la instalación de aplicaciones personales o de programas de comunicación personal, sin que el hecho de haber accedido a la información o mensajes personales del trabajador traiga consigo la nulidad de las pruebas obtenidas respecto de la transgresión de la buena fe contractual y del abuso de confianza.
- A la misma conclusión cabe llegar respecto de los dispositivos electrónicos de uso individual del trabajador, cuando el examen pericial se limita a constatar la existencia de archivos y/o registros que acrediten, atendiendo a la normativa empresarial, el uso indebido del dispositivo llevado a cabo por el trabajador. En otras palabras, el examen pericial no puede extenderse al contenido concreto de los mensajes o correos electrónicos de cuentas privadas, y, aun en el caso de tratarse de la cuenta de correo corporativo, no cabe vulnerar el derecho a la intimidad del trabajador.
- Por último, el procedimiento de investigación debe documentarse de la forma más detallada posible y ha de garantizar una correcta cadena de custodia, de forma que se garantice que los dispositivos incautados no han sido manipulados

y que los resultados del análisis se corresponden con el contenido del dispositivo en el momento exacto en que dejó de estar en posesión del trabajador[74].

2. Prueba del hecho electrónico

La LEC es la norma procesal que con mayor detalle desarrolla los medios de prueba, de hecho, ni la LECrim ni la LRJS contienen artículos dedicados a los medios de prueba de los que las partes puedan valerse en los respectivos órdenes jurisdiccionales. Así pues, en la medida en que el artículo 4 LEC determina que las disposiciones de dicha Ley serán supletorias respecto de las establecidas en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, el presente apartado se centrará en la regulación habida a este respecto en el orden civil.

El hecho electrónico puede introducirse en el proceso por cualquiera de los medios de prueba previstos en el artículo 299.1 y 2 LEC. En este sentido, dependiendo de la naturaleza o manifestaciones del hecho y de aquello que se quiera probar, se optará por uno u otro medio de prueba, teniendo en cuenta la posibilidad de que distintos medios de prueba se complementen entre sí. De esta forma, resulta conveniente el empleo de distintos medios probatorios para reforzar la prueba del hecho electrónico con el fin de alcanzar el convencimiento del juez o tribunal.

2.1 La prueba documental

En este caso, habrá que diferenciar según la prueba del hecho electrónico se introduzca en el proceso mediante prueba documental pública o privada[75].

En cuanto a los documentos públicos, es posible introducir en el proceso mensajes de WhatsApp o correos electrónicos, por ejemplo, a través de un acta notarial de exhibición de cosas o documentos (artículo 207 RN)[76]-[77]. Esta acta de exhibición

[74] Véase a este respecto RICHARD GONZÁLEZ, M. "Requisitos y límites de la investigación preprocesal y prueba pericial sobre dispositivos electrónicos de la empresa usados por el empleado", en *Diario LA LEY*, 2017, en el que se explica el procedimiento técnicamente impecable seguido en el caso resuelto por la sentencia del Tribunal Superior de Justicia de Madrid de 13/05/2016, núm. 407/2016 (Aranzadi), aunque dichas evidencias quedaron anuladas por el TSJ al haberse obtenido accediendo a una cuenta de correo electrónico personal del trabajador.

[75] En relación con las clases de documentos, me remito a lo explicado en el apartado relativo al "*Documento electrónico*".

[76] El contenido de las actas notariales se refiere a la constatación de hechos o la percepción que de los mismos tenga el Notario, siempre y cuando no se califiquen como actos y contratos, así como sus juicios

contendrá, entre otras cosas, la transcripción de los mensajes, la hora y fecha de los mismos, el modelo y marca del terminal, el número de teléfono de los intervinientes en la comunicación y la identidad de la persona que solicite el levantamiento de acta en relación a los mensajes y la fecha en que lo hace.

Otra posibilidad la constituye el acta de presencia, la cual acredita la realidad o verdad del hecho que motiva su autorización (artículo 199 RN). Un particular puede mostrar al notario una serie de imágenes, archivos o datos que consten en un dispositivo electrónico, o solicitarle que observe el contenido de una determinada página web o los mensajes habidos en la bandeja de entrada de su cuenta de correo electrónico. Así, teniendo en cuenta los detalles que interesen al requirente, el notario redactará en uno o varios actos lo que presencie o perciba por sus propios sentidos, incorporando al acta la impresión de los correos electrónicos, página web, imágenes, archivos o datos.

En los dos casos anteriores, las actas notariales no podrán extenderse a aquellos aspectos que requieran de conocimientos periciales, por lo que no podrán certificar la ausencia de manipulación o alteración de los mensajes o documentos, es decir, no garantizan la integridad de los mismos (salvo que intervenga un perito informático). En cualquier caso, el acta no deja de ser un documento público con valor tasado, lo que es de gran relevancia a efectos probatorios.

Por otro lado, como complemento a las actas referidas, cabe levantar acta de depósito (artículo 216 RN) que garantice la cadena de custodia de los mensajes u otros hechos producidos en medios electrónicos que hayan sido objeto de dichas actas. De este modo, se posibilita que la parte contraria efectué su propio dictamen pericial sobre los mismos mensajes o datos. Así sucede, en el marco del proceso social, en el caso resuelto por la sentencia del Tribunal Superior de Justicia de Madrid de 13/05/2016, núm. 407/2016.

---

o calificaciones (artículo 17 LN). La fe pública notarial en la esfera de los hechos determina la exactitud de lo que el notario ve, oye o percibe por sus sentidos (artículo 1 RN).

[77] Artículo 207 RN: «*En las actas de exhibición de cosas, el Notario describirá o relacionará las circunstancias que las identifiquen, diferenciando lo que resulte de su percepción de lo que manifiesten peritos u otras personas presentes en el acto, y podrá completar la descripción mediante planos, diseños, certificaciones, fotografías o fotocopias que incorporará a la matriz. En las actas de exhibición de documentos, además, transcribirá o relacionará aquéllos o concretará su narración a determinados extremos de los mismos, indicados por el requirente, observando en este caso, si a su parecer procede, lo dispuesto en el párrafo último del artículo 237*».

Asimismo, el Letrado de la Administración de Justicia podrá dar fe pública judicial del documento o imagen en que haya quedado plasmado el hecho electrónico (artículo 145.1.1º LEC). A modo de ejemplo, en el caso de mensajes producidos en una aplicación de mensajería instantánea como WhatsApp, se trataría de aportar el teléfono móvil en el que se aloje la conversación y la transcripción escrita de la misma para que el LAJ certifique la correspondencia entre ambas. En esta diligencia de cotejo, con carácter general, el LAJ levantará acta consignando la identidad de la persona que muestra su teléfono móvil, el modelo de teléfono y el número correspondiente, así como el número de la persona o personas con las que mantiene la conversación y, en su caso, declarará la correspondencia de lo observado en el teléfono móvil con la transcripción de los mensajes recibidos en el terminal y la confirmación de que estos se corresponden con el número y el teléfono[78]. No obstante, al igual que en el caso anterior el acta solamente acredita la existencia de la comunicación, pero no su integridad.

De igual modo, nada impide a las partes imprimir un e-mail, los "pantallazos" de conversaciones en aplicaciones de mensajería instantánea o una página web e incorporarlos al proceso como prueba documental privada[79]. Para estos casos, el artículo 267 LEC dispone que deberá presentarse en *«original o mediante copia autenticada por el fedatario público competente y se unirán a los autos o se dejará testimonio de ellos,*

[78] En este sentido, cabe citar la sentencia de la Audiencia Provincial de Córdoba de 02/04/2014, núm. 159/2014 (Aranzadi), que recoge un supuesto en el que el Letrado de la Administración de Justicia levantó acta acerca del contenido de los mensajes con su transcripción, estableciendo la correspondencia de estos con el número de teléfono y con el teléfono móvil: «*según consta en la diligencia extendida por el mismo el 20 de diciembre de 2.013 (folio 44), procediera a la "transcripción xerográfica de los mensajes recibidos por doña Dolores en el terminal número NUM003 "*
Por tanto, del propio texto de la diligencia resulta que quien ostentaba la fe pública judicial, ejercitada dentro del marco de lo dispuesto en el artículo 453 de la Ley Orgánica del Poder Judicial (RCL 1985, 1578 y 2635) , con carácter exclusivo y pleno, dejó constancia de un hecho con trascendencia procesal. Nada hay que objetar a un acto consistente en reflejar, merced a una serie de fotocopias de las diversas pantallas del terminal presentado por la denunciante, determinados mensajes a través de "Whatsapp" asociados a un usuario con nombre " Jose Miguel ", el del denunciado, incorporadas a los autos entre los folios 46 y 78.
Como es lógico, la parte personada tiene derecho a concurrir a cualquier acto procesal, pero dicha legitimación no implica que su ausencia haya de privar necesariamente de valor a dicha diligencia de constancia, garantizado como está por el fedatario público, no solo el contenido de lo que se le mostró, sino todas las circunstancias que percibió, hasta el punto de que están reproducidas de manera que cualquier persona puede volver a constatarlas, mediante las correspondientes fotocopias».

[79] Debe señalarse, eso sí, que en estos casos es recomendable proponer prueba testifical al objeto de complementar y reforzar dicha prueba. Así se deduce de la sentencia de la Audiencia Provincial de Barcelona de 06/09/2016, núm. 486/2016 (Aranzadi), la cual se pronuncia negando el valor probatorio de un documento con la transcripción de unos mensajes de WhatsApp. En el caso enjuiciado la parte actora cuestiono la autenticidad de los mensajes, no hubo cotejo por parte del LAJ y, como dice la sentencia, *«aunque no propusiera prueba pericial informática acerca de la autenticidad de los mensajes, bien pudo, al menos, haber propuesto el interrogatorio de la actora, a fin de que reconociese la autoría o no de los mensajes que le era atribuida de contrario»*.

con devolución de los originales o copias fehacientes presentadas, si así lo solicitan los interesados»[80]. Si solamente se dispone de copia simple del documento privado, podrá presentarse esta, surtiendo los mismos efectos que el original siempre y cuando las demás partes no cuestionen la conformidad de la copia con el original.

Por otro lado, las partes pueden optar por introducir una impresión en papel acompañada de un certificado de firma electrónica de una empresa dedicada a la certificación de comunicaciones electrónicas, del contenido de páginas web o redes sociales, fotografías, etc. Este tipo de servicios permiten acreditar la comunicación electrónica y su contenido a través del empleo de la firma electrónica avanzada (artículo 3.2 LFE), lo cual permite la identificación del firmante y detectar cualquier cambio posterior en los datos firmados. De forma adicional, estas empresas emplean el "sello de tiempo" o *timestamp* que garantiza fehacientemente que una serie de datos han existido en un momento determinado y que no han sido modificados desde el momento en que se firmó el documento[81]. A pesar de que estos mecanismos únicamente aseguran la integridad de la prueba con posterioridad a su empleo, pueden ser de gran utilidad a efectos probatorios.

En todo caso, hay que señalar que tanto los documentos públicos como privados permiten la incorporación al proceso de documentos electrónicos (artículos 267 y 268 LEC), que en el caso de los documentos públicos se efectuará por medio de una imagen digitalizada incorporada como anexo y firmada mediante firma electrónica reconocida, y en el caso de los documentos privados a través de imágenes digitalizadas, incorporadas a anexos firmados electrónicamente. Otra cuestión relevante que afecta a ambos tipos de documentos, son las consecuencias derivada de la comprobación de la autenticidad o exactitud de la copia o testimonio impugnados, que no es otro que

[80] Una forma de aportar el original en sede judicial será guardando las conversaciones de la aplicación de mensajería instantánea en un USB, manteniendo los mensajes en su formato original.

[81] El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, contiene en su anexo Glosario de términos una definición del "sello de tiempo" según la cual el mismo consiste en «*La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento*». Este servicio solo puede ser prestado por Autoridad de Sellado de Tiempo o Time Stamp Authority (TSA) que actúa como tercera parte de confianza.

imponer las costas, gastos y derechos que se originen a cargo de quien hubiese formulado la impugnación (artículos 320 y 326 LEC)[82].

En el ámbito del proceso laboral, se han establecido una serie de pautas necesarias para la aportación al proceso de las conversaciones de WhatsApp en forma de documento (sentencia del Tribunal Superior de Justicia de Galicia de 28/01/2016, núm. 556/2016). No será suficiente con aportar la impresión en papel de distintas pantallas o "pantallazos" del teléfono móvil, sino que también se reputa necesaria la transcripción de la conversación y la verificación de que esta se corresponde con el teléfono y con el número correspondientes. En este sentido, en la misma línea de lo establecido en párrafos anteriores, la jurisprudencia citada sugiere en relación al caso objeto de enjuiciamiento que ello podría haberse conseguido *«a través de la aportación del propio móvil del Sr. Abel y solicitando que, dando fe pública, el LAJ levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y de que éste se corresponde con el teléfono y con el número correspondientes; o incluso, mediante la aportación de un acta notarial sobre los mismos extremos»*. El hecho de que estos "pantallazos" tengan la consideración de prueba documental tiene especial relevancia en el proceso social, pues en el ámbito de la prueba el recurso de suplicación únicamente puede tener por objeto las pruebas documentales y periciales practicadas (artículo 193 b) LRJS)[83].

[82] Más aun, el tribunal puede llegar a imponer un multa de 120 a 600 euros, o de 300 a 1.200, según los casos, si aprecia que la impugnación fue temeraria.

[83] No obstante, a este respecto existen algunos pronunciamientos que rechazan la consideración de los mensajes de WhatsApp como documentos. A este respecto cabe citar la sentencia del Tribunal Superior de Justicia de Andalucía de 17/06/2020, núm. 1629/2020 (Aranzadi), o la del Tribunal Superior de Justicia de Galicia de 5/06/2020, núm. rec. 3815/2019 (Aranzadi), declarando que *«No se admite la revisión fáctica interesada del referido hecho probado primero por lo siguiente (1) Se trata de hechos que aparecen contradichos por otros medios de prueba, en efecto, la parte recurrente pretende apoyar la revisión del hecho probado en la documental consistente en transcripciones de correo de whatsApp, pero los whatsApps no son prueba documental al no tener la condición de documento informático ni electrónico, así lo tiene declarado este Tribunal, entre otras, en la Sentencia de 26 de marzo de 2019 (AS 2019, 2129) (RSU 440/2019), en la que declaramos que la prueba testifical no está incluida dentro de los medios de prueba recogidos en el art. 193 b) de la LRJS (RCL 2011, 1845) , y un whatsapp, a pesar de que la actora lo aporta como prueba documental, no es prueba documental. Los whatsapp- servicio de mensajería instantánea - es uno de los nuevos medios de prueba a los que se refiere el art. 299.2 de la LEC (RCL 2000, 34, 962 y RCL 2001, 1892) frente a los medios de prueba tradicionales a los que se refiere el art. 299.1 de la LEC, , y la prueba documental, que es la recogida en el art. 193 b) con eficacia revisoría, está recogida dentro de los medios de prueba tradicionales (en concreto puntos 2 y 3 del art. 299 LEC»*. En sentido contrario, la sentencia del Tribunal Supremo de 23/07/2020, núm. 706/2020 (Aranzadi), se muestra en favor de un concepto amplio de documento concluyendo que *«El avance tecnológico ha hecho que muchos documentos se materialicen y presenten a juicio a través de los nuevos soportes electrónicos, lo que no debe excluir su naturaleza de prueba documental, con las necesarias adaptaciones (por ejemplo, respecto de la prueba de autenticación). Si no se postula un concepto amplio*

En todo caso, queda claro que el valor probatorio de la prueba documental en la que consta el "pantallazo" dependerá de las circunstancias concurrentes en cada caso. Así se deduce de lo declarado por el TSJ de Galicia como continuación del extracto previamente citado, en el que enumera cuatro supuestos en los que se aceptaría una conversación de este tipo como documento: *«(a) cuando la parte interlocutora de la conversación no impugna la conversación; (b) cuando reconoce expresamente dicha conversación y su contenido; (c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición); o, finalmente, (d) cuando se practique una prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores»*. Como puede observarse, es perfectamente posible recurrir a la prueba documental para aportar unos mensajes o correos al proceso, dado que si la parte contraria no impugna la veracidad de lo volcado en soporte impreso puede considerarse que admite su contenido. En caso contrario, se produce un desplazamiento de la carga de probar la autenticidad e integridad de los mensajes o correos a la parte que los aportó, que deberá valerse de medios de prueba instrumentales como la prueba pericial[84].

Por otra parte, en el proceso penal, podrá presentarse como prueba documental la transcripción de los fragmentos más relevantes de las grabaciones derivadas de la intervención de las comunicaciones telefónicas, correspondiendo a la defensa, que habrá conocido previamente su contenido, solicitar su audición total o parcial en el acto del juicio. En este sentido, la sentencia del Tribunal Supremo de 04/02/2015, núm. 23/2015, afirmó que las conversaciones intervenidas pueden incorporarse al proceso por distintos medios probatorios, como la testifical de los funcionarios policiales que llevaron a cabo la diligencia de investigación o como prueba documental mediante su trascripción mecanográfica[85]. Dicho esto, la sentencia añade que dicha prueba documental puede

---

de prueba documental, llegará un momento en que la revisión fáctica casacional quedará vaciada de contenido si se limita a los documentos escritos, cuyo uso será exiguo. En consecuencia, debemos atribuir la naturaleza de prueba documental a los citados correos electrónicos obrantes a los folios 730, 731 y 505 de las actuaciones».

[84] La autenticidad de unos mensajes o correos se refiere a la coincidencia entre autor aparente de los mismos con su autor real, supone garantizar de la autenticidad del origen de los datos; mientras que la integridad de los mensajes o correos alude a su preservación, es decir, que los mismos no han sido alterados o manipulados de forma no autorizada.

[85] RICHARD GONZÁLEZ señala que la declaración de los agentes intervinientes puede ser útil para complementar la prueba documental ya que podrán dar cuenta de cómo se llevó a cabo la intervención, qué oyeron o vieron, pudiendo resultar fundamental para comprender conversaciones en las que se empleen nombres o palabras clave, en RICHARD GONZÁLEZ, M. *Investigación y prueba mediante medidas*

darse por reproducida *«siempre que dicha prueba se haya conformado con las demás garantías y se haya podido someter a contradicción y que tal proceder, en suma, no conlleve una merma del derecho de defensa»*. Por ello, su inclusión en el acervo probatorio como prueba documental, requiere que la medida haya sido autorizada y contralada por el juez, que las grabaciones y las transcripciones hayan sido debidamente cotejadas bajo la fe pública del LAJ y que las cintas originales estén a disposición de las partes, es decir, debe ser procesalmente intachable.

2.2 La prueba pericial

La prueba pericial es un medio probatorio mediante el cual el perito aporta al órgano judicial sus conocimientos científicos, artísticos, técnicos o prácticos en caso de que resulten necesarios para valorar hechos o circunstancias relevantes en el proceso o para acreditar los mismos[86]. Este medio probatorio podrá tener por objeto garantizar la autenticidad e integridad de otras pruebas cuando estas hayan sido impugnadas de la parte contraria (prueba complementaria), o bien ilustrar al órgano judicial sobre aspectos no aprehensibles por los sentidos y que requieran de conocimientos específicos (prueba autónoma)[87]. De este modo, la prueba pericial informática aportará al proceso la información técnica o científica relativa al hecho o a la manifestación del hecho electrónico que el resto de medios probatorios no alcanzan, sin que por ello se convierta en el único medio probatorio capaz de convencer al juzgador de la autenticidad e integridad de la prueba[88]. En todo caso, para poder ser valorada como prueba y en

---

de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido, Wolters Kluwer, Madrid, 2017, pág. 322.

[86] La designación del perito podrá realizarse por las partes o por el tribunal en alguno de los supuestos previstos en el artículo 339 LEC. Una de las diferencias entre ambos es que los peritos designados por las partes podrán ser tachados, mientras que los designados judicialmente, en su caso, serán objeto de recusación (artículo 343 y 344 LEC).

[87] En relación con la titulación necesaria para confeccionar un dictamen de esta naturaleza, en la actualidad no existe una normativa de ámbito nacional o internacional que especifique la titulación o conocimientos necesarios al efecto. En lo que respecta al proceso civil, el artículo 340.1 LEC exige que los peritos posean el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste, pero si se trata de materias comprendidas en títulos profesionales oficiales, autoriza a nombrar como perito a personas entendidas en aquellas materias. Asimismo, prevé la posibilidad de que el dictamen pericial se emita por Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia, así como por personas jurídicas legalmente habilitadas para ello (artículo 340.2 LEC). En el ámbito del proceso penal, se distingue entre peritos titulares y no titulares, teniendo preferencia los primeros (artículos 457 y 458 LECrim). Por ello, algunos autores han entendido que un perito que emita dictámenes en esta materia debería estar graduado en informática, ingeniería informática, telecomunicaciones o matemáticas. Sobre este tema, véase PINTO PALACIOS, F. y PUJOL CAPILLA, P. "La prueba pericial informática", en *Diario La Ley*, núm. 5, 2017, págs. 3-6.

[88] RICHARD GONZÁLEZ explica a este respecto que *«se trata de una prueba pericial ordinaria que se distingue por su contenido que será el del análisis de programas, sistemas de comunicación, archivos*

cumplimiento de los principios de inmediación y contradicción, la prueba pericial deberá ratificarse por el perito (o por algún perito del mismo equipo) en el acto del juicio[89].

DELGADO MARTÍN recuerda que la pericial informática puede referirse a dos modalidades básicas de datos, en concreto, a los almacenados en dispositivos de naturaleza electrónica y los transmitidos por redes de comunicación. En lo que respecta a los primeros, el autor distingue tres tipos de soportes[90]:

1) Soportes informáticos: este grupo a su vez se divide en los soportes portátiles y los contenidos en equipos portátiles o de sobremesa. A los primeros los define como aquellos que disponen de una carcasa que permite su traslado garantizando la integridad del contenido (memory stick, SD card, dispositivos USB como el pendrive, MP3, discos duros externos,…). En relación a los segundos, se refiere principalmente a los discos duros situados en el interior de los equipos informáticos.
2) Terminales de telefonía móvil: tanto la memoria interna del teléfono como la tarjeta SIM, incluyendo la memoria externa adicional que pudiera tener el teléfono como soporte informático portátil.
3) Otros dispositivos electrónicos: este grupo lo integran cualesquiera otros dispositivos electrónicos capaces de almacenar información, como por ejemplo lectores de bandas magnéticas, tarjetas de televisión de pago, GPS, etc.

En el caso de los mensajes de WhatsApp volcados en papel, la labor del perito informático consistirá en examinar el teléfono móvil u otro dispositivo electrónico (un ordenador) mediante el cual se hayan enviado o recibido los mensajes, descartando o confirmando la concurrencia de algún tipo de manipulación en la autenticidad del origen y la integridad de los mensajes. En el terreno práctico, la prueba pericial podría emplearse, por ejemplo, para acreditar la identidad de los interlocutores y la integridad de los mensajes en los que se reconozca una deuda. Con todo, acreditar la autoría de unos mensajes por esta vía puede resultar complicado pues, pese a que en ocasiones se

informáticos de cualquier clase y, en general, todos aquellos hechos que se produzcan, transmitan o manifiesten en forma electrónica» en RICHARD GONZÁLEZ, M. *Investigación y prueba mediante medidas de…, ob. cit.*, 2017, pág. 329.

[89] Con la excepción prevista en el artículo 788.2 LECrim en el ámbito del procedimiento abreviado, según la cual dicho informe pericial tendrá carácter de prueba documental.

[90] DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital…, ob. cit.,* 2016, pág. 66.

necesita un código de desbloqueo, estos son transferibles o pueden ser conocidos por otras personas que pueden haber enviado los mensajes. Por este motivo, en muchas ocasiones la autoría de los mensajes vendrá deducida de la valoración conjunta de la prueba.

En lo que se refiere a los correos electrónicos impresos en papel, el perito informático no solo analizará la cuenta de correo electrónico y el soporte utilizado para enviar los correos electrónicos, sino que además deberá hacer lo propio con la cuenta de correo electrónico y el dispositivo electrónico de destino para acreditar la autenticidad del origen y la integridad del contenido[91]. Se trata de probar la autenticidad e integridad de los elementos que configuran el e-mail, es decir, el remitente, destinatario o destinatarios, el asunto, el contenido, los documentos adjuntos, los metadatos, etc. Ahora bien, tal y como explica GOÑI IRULEGUI, el perito informático se enfrentará con dos grandes dificultades al analizar los correos electrónicos aportados en papel: por un lado, si se desea certificar la salida y recepción en destino de un correo electrónico, ello no puede garantizarse únicamente a partir del análisis del correo enviado, sino que será necesario efectuar un análisis forense de los servidores de salida y destino, pero normalmente esto no es posible. Por otro lado, en cuanto al contenido del mensaje enviado, en la mayoría de los casos no es posible acceder al mismo porque los servidores de correo electrónico no almacenan el contenido del mensaje una vez este es entregado, dejando constancia solamente de unas trazas o apuntes del origen y del destinatario, así como de los instantes de recepción y entrega[92].

En el marco del proceso penal, las evidencias obtenidas por medio de las diligencias de investigación tecnológicas de interceptación de las comunicaciones telemáticas, o de registro (remoto o no) de dispositivos de almacenamiento masivo de la

[91] CAPEÁNS AMENEDO alude a la verificación de correos electrónicos, junto con el informe pericial sobre ordenadores, el análisis de la manipulación de archivos audiovisuales y la certificación de desarrollo de software, como las periciales informáticas más habituales en el ámbito laboral, en CAPEÁNS AMENEDO, C. *Derecho del trabajo y nuevas tecnologías. Conflicto entre las tecnologías de información y comunicación y el derecho a la intimidad y propia imagen.* Colex, A Coruña, 2020.

[92] La autora basa su explicación en lo declarado por la sentencia del Juzgado de lo Social nº3 de Pamplona, de 31/03/2017, núm. 74/2017 (Aranzadi), de la que igualmente cabe destacar que *«"aportar un correo electrónico recibido original es algo prácticamente impracticable desde el punto de vista técnico . Para ello, sería necesario adjuntar al procedimiento el disco duro del servidor al que llegó el correo electrónico, con su correspondiente código hash calculado ante fedatario público, suponiendo que la configuración del servidor conserve los correos electrónicos en el mismo una vez éstos han sido entregados a sus destinatarios"»,* en PICÓ I JUNOY, J., ANDINO LÓPEZ, J.A. y CERRATO GURI, E. *La prueba pericial a examen. Propuestas de lege ferenda*, Bosch, Barcelona, 2020, pág. 539.

información, se incorporarán al proceso mediante informe pericial como prueba fundamental del resultado de la intervención, sin perjuicio de que se practique la prueba prevista en el artículo 299.2 LEC. A estos informes policiales elaborados por agentes expertos se les ha denominado como periciales de inteligencia, como una variante tanto del artículo 456 LECrim como del 335 LEC. En cualquier caso, se ha llegado a considerar como una prueba mixta pericial/testifical, por cuanto los policías podrán comparecer en calidad de autores del informe pericial o como testigos de la investigación[93].

La elaboración de un informe pericial que dé cuenta de la autenticidad e integridad del hecho electrónico con todas las garantías puede ser complejo, lento y costoso, razón por la que en muchas ocasiones se opta por el volcado de los mensajes en papel. En esta tesitura, resulta habitual tratar de reforzar dicha prueba mediante la testifical del otro interlocutor, de una persona que presenció la comunicación o de alguien que vio que una página web publicada un producto o contenido; o a través del reconocimiento judicial del teléfono móvil, *tablet* u otro dispositivo electrónico para que el juez constate el contenido de una página web, de una conversación producida por medios electrónicos, la identidad de los interlocutores, etc[94].

En esta línea, la sentencia del Tribunal Supremo de 19/05/2015, núm. 300/2015, a pesar de reconocer el riesgo de manipulación de los archivos digitales, aludiendo al anonimato que permiten estos sistemas y a la facilidad de crear cuentas con una identidad fingida, admite la prueba documental consistente en una fotografía que la Guardia Civil hizo a la pantalla del teléfono de la víctima[95]. En relación con la problemática expuesta, si bien el tribunal subraya la indispensable necesidad de practicar una prueba pericial ante la impugnación de la autenticidad e integridad de la conversación, finalmente otorga pleno valor probatorio a la prueba impugnada sin necesidad de aportar informe pericial con base en: la declaración como testigo del

[93] A modo de ejemplo, la sentencia del Tribunal Supremo de 07/02/2019, núm. 65/2019 (Aranzadi).

[94] El reconocimiento judicial puede practicarse de oficio o a instancia de parte, como prueba autónoma o, como se ha dicho, conjuntamente con otro medio de prueba. Cuando se practique conjuntamente con la prueba pericial, ambos medios de prueba se practicarán simultáneamente de forma que el juez navegue por la red u observe el contenido de un dispositivo electrónico mientras el perito da las explicaciones oportunas. En caso de que se practique conjuntamente con el interrogatorio de las partes y/o testigos, se hará de forma sucesiva, practicándose en primer lugar el reconocimiento judicial, pasando a continuación a la declaración de las partes y/o de los testigos.

[95] Dicha imagen mostraba la conversación de la víctima con un amigo en Tuenti Messenger en la que le narraba los hechos objeto del proceso (abusos sexuales por parte de la pareja de su madre).

amigo de la víctima que confirmó tanto haber mantenido dicha conversación como su contenido, la declaración de los agentes de la Guardia Civil y el principio de disponibilidad y facilidad probatoria (ya que la víctima puso a disposición del juez su contraseña de Tuenti con el fin de posibilitar, llegado el caso, la comprobación de la autenticidad de dicha conversación mediante el correspondiente informe pericial)[96].

Grosso modo, puede afirmarse que, si bien la prueba pericial siempre servirá para reforzar la posición procesal, la necesidad de llevarla a cabo vendrá condicionada por las circunstancias del caso, el conjunto de las pruebas de que se disponga y de la postura procesal de la parte contraria. Que la prueba del hecho electrónico o de los hechos producidos en medios electrónicos sea manipulable, por ejemplo, suprimiendo parte o alterando datos, no implica que la prueba pericial se convierta en un medio probatorio indispensable en todos los casos. Mucho menos teniendo en cuenta que no es el único medio probatorio susceptible de ser manipulado o falsificado[97].

2.3 Reproducción de la palabra, sonido e imagen y los instrumentos que permiten archivar y conocer datos

Las imágenes, palabras o sonidos grabados en medios no digitales (video VHS, grabaciones en casete,…), que en la actualidad constituyen tecnologías en desuso, se incorporarán al proceso por la vía de los artículos 382 y 383 LEC; mientras que los grabados en formato digital (imagen de fotografía digital, grabación de video en formato digital almacenada en DVD,…) lo harán por la vía del artículo 384 LEC. De otro lado, las palabras, datos, cifras y operaciones matemáticas archivadas en instrumentos que permitan archivar, conocer o reproducirlas o en documentos electrónicos (artículo 8 LFE), se incorporarán al proceso de acuerdo con lo dispuesto en el artículo 384 LEC.

---

[96] Véase DELGADO MARTÍN, J. "La prueba del whatsapp", en *Diario La Ley*, núm. 8605, 2015.

[97] Un claro reflejo de esta realidad lo constituyen los delitos de falso testimonio (*ex* artículo 458 CP) o falsedad documental (*ex* artículo 390 y ss. CP). Como advierte la sentencia del Tribunal Supremo de 19/07/2018, núm. 375/2018 (Aranzadi) *«No es posible entender, como se deduce del recurso, que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad -por la existencia de sospechas o indicios de manipulación- se debe realizar tal pericia acerca del verdadero emisor de los mensajes y su contenido. Ahora bien, tal pericia no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba».*

La parte que proponga este medio de prueba deberá cerciorarse de que el tribunal dispone del medio técnico necesario para la práctica de la prueba, pues en caso de no disponer del mismo será ella la que deba aportarlo a fin de posibilitarla. Asimismo, en caso de proponer el medio de prueba de reproducción de la palabra, sonido e imagen del artículo 382 LEC, la parte deberá acompañar, en su caso, la transcripción escrita de las palabras contenidas en el soporte de que se trate y que sean relevantes para el caso. ORMAZÁBAL SÁNCHEZ recomienda, en relación con lo anterior, que en la proposición de la prueba se especifique qué fragmento o parte pretende emplearse como prueba cuando las imágenes o sonidos del medio audiovisual sean de larga duración[98].

Nótese que, además, la ley contempla la posibilidad de que la parte que proponga este medio de prueba aporte dictámenes periciales y cualesquiera otros medios de prueba instrumentales que considere convenientes a su derecho, si bien reconoce la misma facultad a la parte contraria para poder cuestionar la autenticidad o exactitud de lo reproducido. Al mismo tiempo, cabe destacar una especialidad de la prueba de instrumentos recogida en el artículo 384.1 LEC, que se refiere a que estos serán examinados por el tribunal con los medios que la parte proponente aporte, con los que el tribunal disponga de oficio y con los que en su caso aporte la parte contraria. Por tanto, el precepto habilita al órgano judicial para practicar de oficio, si así lo precisa, prueba pericial para valorar los instrumentos de archivo, conocimiento o reproducción de datos.

Se trata pues del medio de prueba adecuado, por ejemplo, para aportar al proceso los datos o informaciones contenidos en dispositivos electrónicos que pueden resultar inapreciables en caso de imprimirse y aportarse como prueba documental. De este modo, en ambos casos se precisa de un acto de reproducción que haga visualizable o audible su contenido para que pueda ser aprehendida por el entendimiento humano.

Respecto de las grabaciones derivadas de la medida de intervención telefónica, la sentencia del Tribunal Supremo de 13/04/2016, núm. 307/2016, declara que la reproducción directa de las grabaciones en el plenario solventa las insuficiencias de formalización y transcripción que pudieran producirse en la fase de instrucción. Cuando

[98] ORMAZÁBAL SÁNCHEZ, G. *La prueba documental y la prueba mediante soportes informáticos*, Wolters Kluwer, Madrid, 2019, pág. 181.

se proceda llevar a cabo un reconocimiento de las voces de los acusados mediante su audición (y visión de la grabación), salvo que alguna de las partes cuestione la identidad de las voces solicitando a tal efecto que se lleve a cabo una pericial de cotejo de las mismas, el tribunal por sí mismo puede reconocer la voz de grabada e identificarla con la del acusado (sentencia del Tribunal Supremo de 07/12/2001, núm. 2384/2001).

3. Valoración de la prueba del hecho electrónico

3.1 La prueba ilícita en el proceso

La prueba ilícita se refiere a la prueba obtenida o incorporada al proceso con vulneración de derechos fundamentales, cuya consecuencia fundamental es la nulidad absoluta o de pleno derecho de la misma[99]. Ello supone que la prueba así obtenida no desplegará ningún efecto en el proceso ni podrá ser subsanada o convalidada de ninguna forma, y en caso de que haya sido incorporada al proceso deberá ser excluida del mismo. Este sistema se justifica en base a dos fundamentos: de un lado, se busca producir un efecto disuasorio que sirva para prevenir este tipo de prácticas en la investigación penal; de otro lado, la supremacía de los derechos fundamentales conlleva la prohibición del reconocimiento judicial de las pruebas ilícitamente obtenidas, y ello pese a que la Constitución no recoge un derecho autónomo que impida la admisión jurisdiccional de este tipo de pruebas con origen antijurídico.

El artículo 11.1 LOPJ positivizó la ilicitud de la prueba en estos casos afirmando que «*No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*»[100]. Como puede observarse, en la redacción

[99] Ello la diferencia de la prueba irregular, la cual se corresponde con la prueba en cuya obtención o práctica se han infringido preceptos de ley ordinaria o de normativa procesal. Esta prueba puede llegar a ser declarada nula, pero en este caso no arrastrará consigo al resto de los medios de prueba que deriven de aquella.

[100] Debe señalarse que la prueba ilícita en el sentido que aquí se ha explicado apareció por primera vez en la sentencia del Tribunal Constitucional de 29/11/1984, núm. 114/84 (Aranzadi), en un momento en que, como la propia sentencia afirma, no existía norma legal que determinara la interdicción procesal de la prueba ilícitamente obtenida. Adicionalmente, cabe mencionar que en un primer momento el Tribunal Constitucional entendía que las sentencias condenatorias con base a pruebas de cargo obtenidas con violación de derechos fundamentales suponían una vulneración del derecho a la presunción de inocencia, lo que traía consigo la anulación de la sentencia de instancia y la absolución del acusado. Sin embargo, a partir de la sentencia del Tribunal Constitucional de 05/04/1999, núm. 49/1999 (Aranzadi), el órgano constitucional ha pasado a entender que la vulneración de derechos fundamentales en la obtención de la prueba implica la vulneración del derecho fundamental a un proceso con todas las garantías, y, en este caso, el Tribunal Constitucional podría decretar la nulidad del juicio oral y la retroacción de las actuaciones al momento en que se produjo la vulneración, llevándose a cabo un nuevo trámite

del precepto el legislador introdujo no solo la teoría directa, que se correspondería con lo hasta ahora comentado, sino que también añadió la teoría indirecta o refleja conocida igualmente como la doctrina de los frutos del árbol envenenado. En virtud de esta última doctrina, la ilegitimidad alcanza tanto a la prueba en cuya obtención se han vulnerado derechos fundamentales como a todas aquellas pruebas que, a pesar de haberse obtenido lícitamente, están basadas o derivan de la obtenida de forma ilícita.

A pesar de lo anterior, lo cierto es que esta aparente rigidez con la que se caracteriza la regla de exclusión se ha ido relajando paulatinamente a través de la creación de diversas excepciones que limitan el alcance y los efectos de esta regla. Encontramos una primera excepción en la llamada prueba independiente, que a diferencia de la prueba diferente pero derivada de la prueba obtenida vulnerando derechos fundamentales, es una prueba válida que no guarda relación con la prueba ilícita, lo cual impide que la misma se vea arrastrada por los efectos indirectos de la ilicitud.

Asimismo, dentro de estas excepciones se encuentran las conocidas como "el descubrimiento inevitable", el "hallazgo casual" y la "buena fe". La primera de ellas se fundamenta en la idea de que, si no se hubiera producido la vulneración del derecho fundamental, la prueba derivada habría sido inevitablemente obtenida durante el curso de la investigación a través de vías respetuosas con los derechos fundamentales. La segunda, por su parte, determina que el descubrimiento de hechos o elementos probatorios de un determinado delito durante el curso de una investigación autorizada para otro delito distinto, respecto del cual se está produciendo una inmisión legitima en los derechos fundamentales afectados, no supone la nulidad de lo descubierto como prueba de cargo del segundo delito. Finalmente, la tercera de las excepciones consiste en admitir aquellas pruebas derivadas, obtenidas con vulneración de derechos fundamentales, cuando el infractor cree estar obrando de acuerdo con el ordenamiento jurídico (buena fe), y no pueda inferirse de los hechos probados que la actuación policial estuviera encaminada a cometer tal vulneración[101].

---

proposición y admisión o inadmisión de la prueba, de cuya valoración se determinará nuevamente la culpabilidad o absolución del investigado.

[101] La sentencia del Tribunal Constitucional de 10/02/2003, núm. 22/2003 (Aranzadi), refleja esta excepción: «*La inconstitucionalidad de la entrada y registro obedece, en este caso, pura y exclusivamente, a un déficit en el estado de la interpretación del Ordenamiento que no cabe proyectar*

Otra excepción, aplicada en numerosas ocasiones por los órganos jurisdiccionales, la constituye la doctrina de la "conexión de antijuridicidad". De conformidad con esta doctrina, el tribunal puede valorar las pruebas derivadas de otras pruebas declaradas ilícitas cuando se consideren jurídicamente independientes y ajenas a las constitucionalmente ilegitimas, aunque entre ellas exista una relación natural de causalidad[102]. Para determinar la concurrencia o no de la conexión de antijuridicidad, el Tribunal Constitucional realiza un examen a partir de dos perspectivas: desde una perspectiva interna, que se refiere a la índole y características de la vulneración del derecho fundamental afectado y al resultado inmediato de la infracción; y, desde una perspectiva externa, relacionada con las necesidades esenciales de tutela que la realidad y efectividad del derecho vulnerado exigen.

Con base a esta teoría, en supuestos en los que se ha declarado la nulidad de un registro domiciliario o de la interceptación de las comunicaciones telefónicas, la jurisprudencia ha considerado que la declaración o reconocimiento de los hechos por parte del acusado se erige como una prueba suficientemente desvinculada de la diligencia inicial ilícita, siempre y cuando se cumplan determinadas condiciones: que la declaración se haya producido de forma distante en el tiempo respecto de la diligencia declarada ilícita, que la misma haya sido realizada con presencia de abogado y con conocimiento de los derechos que le asisten (derecho a guardar silencio, no declarar contra sí mismo o a no confesarse culpable), y que en la declaración puedan apreciarse las notas de espontaneidad y voluntariedad[103]. En este caso, la declaración se entiende

---

sobre la actuación de los órganos encargados de la investigación imponiendo, a modo de sanción, la invalidez de una prueba, como el hallazgo de una pistola que, por sí misma, no materializa en este caso, lesión alguna del derecho fundamental (vid. STC 49/1999, de 5 de abril [RTC 1999, 49] , F. 5) y que, obviamente, dada la situación existente en el caso concreto, se hubiera podido obtener de modo lícito si se hubiera tenido conciencia de la necesidad del mandamiento judicial».

[102] Los críticos con esta doctrina afirman que con el empleo de la misma indirectamente se esta autorizando el uso o aprovechamiento de la información sobre los hechos obtenida a través de pruebas constitucionalmente ilegitimas.

[103] La sentencia del Tribunal Supremo de 30/04/2007, núm. 357/2007 (Aranzadi), afirma en este sentido que: «*El Tribunal Constitucional ha aceptado la validez de la confesión del imputado, siempre que se pueda afirmar que ha sido prestada con todas las garantías y de manera informada y libre. Esta Sala, en algunas sentencias ha entendido que esas condiciones se dan cuando el acusado confiesa los hechos en el juicio oral, pues en ese momento ya conoce las pruebas que la acusación propone como de cargo; ya ha podido tener información acerca del planteamiento de su defensa o de la de otros acusados sobre la validez de las intervenciones telefónicas o sobre las demás pruebas de la acusación; dispone de la necesaria asistencia letrada; ha tenido oportunidad de asesorarse suficientemente acerca de las eventuales consecuencias de la nulidad de las intervenciones telefónicas; ha tenido ocasión de pedir y recibir opinión y consejo técnico acerca de las posibles consecuencias de su confesión; y ha sido informado debidamente de sus derechos, entre los que se encuentra el de no declarar, no confesarse*

fruto de una decisión libre e informada, así como que constituye la manifestación de una elección entre las distintas opciones posibles en el marco de una estrategia procesal de defensa y, por tanto, se convierte en una prueba independiente de la declarada ilícita (no hay conexión de antijuridicidad) y válida para fundamentar una eventual sentencia condenatoria. Por el contrario, no sucede lo mismo cuando se trata de declaraciones sumariales o policiales cercanas a la obtención de la prueba de cargo que luego se declara ilícita por vulneración de derechos fundamentales. En este supuesto se entiende que la declaración del investigado se halla indudablemente condicionada por la prueba ilícita, y que el investigado y su defensa no han tenido la posibilidad de conocer las condiciones en que dicha prueba ha sido obtenida o incorporada al proceso.

En cualquier caso, la declaración de nulidad de la prueba podrá producirse tanto de oficio como a instancia de parte, atendiendo a lo dispuesto en el artículo 240 LOPJ (aplicable a todos los órdenes jurisdiccionales), y de conformidad con la forma en que este regulada la tramitación de este incidente en cada orden jurisdiccional.

3.2 Libre valoración de la prueba

La no vinculación del juzgador a reglas de la prueba tasada, estableciendo que la libre valoración de la prueba, no autoriza a una apreciación discrecional y arbitraria de la prueba, sino que exige la aplicación de criterios racionales conforme a las reglas de la sana crítica. De esta forma, el órgano judicial deberá motivar su convicción con relación a los hechos objeto del proceso y, por tanto, se deberán precisar aquellos criterios y razonamientos que conforme a las reglas de la lógica han llevado al tribunal a una determinada conclusión.

Tal y como se desprende de la regulación de las distintas leyes procesales, el sistema de libre valoración de la prueba será de aplicación con carácter general en todos los órdenes jurisdiccionales. Así se infiere de lo dispuesto en el artículo 97.2 LRJS, al tiempo que el artículo 741 LECrim establece que el tribunal apreciará según su conciencia las pruebas que se practiquen en el juicio y el artículo 218.2 LEC indica que la motivación de las sentencias se ajustará siempre a las reglas de la lógica y de la

---

culpable y no contestar a alguna o alguna de las preguntas que se le hagan. En definitiva, ha tenido oportunidad de decidir cómo orientar su defensa».

razón[104]. En esta línea, la regulación específica de distintos medios de prueba prevé que el tribunal valorará de conformidad con las reglas de la sana crítica, en concreto: el dictamen de peritos (artículo 248 LEC), el interrogatorio de las partes (artículo 316.2 LEC), el interrogatorio de testigos (artículo 376 LEC), los medios de reproducción de la palabra, el sonido y la imagen (artículo 382 LEC) y los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas relevantes para el proceso (artículo 384 LEC).

La prueba pericial se ha considera el medio probatorio más fiable a la hora de probar aquellos aspectos técnicos del hecho electrónico pues, entre otras cosas, es el único medio probatorio capaz de efectuar un análisis de los datos y metadatos en lenguaje informático. A pesar de ello, el juez puede desvincularse de sus razonamientos cuando no los vea lógicos o razonables o crea que el procedimiento seguido no ha sido el adecuado, si bien, claro está, deberá motivar suficientemente esta posición. PICO I JUNOY Y ABEL LLUCH subrayan que «*El juez puede optar por seguir las conclusiones de uno de los dictámenes contradictorios; puede separarse de la opinión de los peritos, aun siendo unánime (STS de 10 de febrero de 1994); puede aceptar en parte y rechazar en parte el dictamen pericial y, a mayor abundamiento, puede preferir la opinión del perito discrepante o simplemente no quedar convencido por ninguno de los dictámenes…*»[105]. Con todo, existen distintos aspectos a tener en cuenta a la hora de valorar la prueba pericial como son la cualificación profesional del perito y su especialización, el método empleado, la proximidad en el tiempo y el carácter detallado del dictamen, etc[106].

De igual forma, en el caso del interrogatorio de las partes, cabe destacar lo dispuesto por los artículos 304, 307 y 316.1 LEC en cuanto a la valoración del interrogatorio de las partes en determinados supuestos. Según se recoge en dichas normas, si la parte citada para el interrogatorio no compareciere al juicio o si habiendo comparecido se negare a declarar o sus respuestas fueran evasivas o inconcluyentes, podrán considerarse reconocidos como ciertos (*ficta admissio*) los hechos en que hubiese intervenido personalmente y su fijación como ciertos le resulte perjudicial en

[104] En términos parecidos el artículo 973 LECrim en sede del procedimiento para el juicio sobre delitos leves.
[105] PICÓ I JUNOY, J., ANDINO LÓPEZ, J.A. Y CERRATO GURI, E. *La prueba pericial a examen…*, ob. cit., 2020, págs. 311-312.
[106] PINTO PALACIOS, F. Y PUJOL CAPILLA, P. *La prueba en…*, ob. cit., 2017, págs. 102-104.

todo o en parte. Misma eficacia se establece cuando, sin contradecir las demás pruebas, una de las partes reconoce hechos en los que intervino personalmente y la fijación de estos como ciertos le es enteramente perjudicial. Sin embargo, lo anterior no será de aplicación al proceso penal puesto que ello resulta incompatible con el derecho a la presunción de inocencia[107]. Ciertamente, previsiones como las de los artículos 304 y 307 LEC chocan frontalmente contra los derechos a no declarar contra uno mismo y a no confesarse culpable. En cualquier caso, los tribunales se regirán por las reglas de la sana crítica en la valoración de las declaraciones de las partes y de las personas a las que se hace referencia en el artículo 301.2 LEC. Todo ello, sin perjuicio de que deba tenerse en consideración la razón de ciencia que hubieren dado, las circunstancias que los rodean y, eventualmente, las tachas que pudieran haberse formulado y los resultados de la prueba sobre estas.

Como se ha venido explicando, la impugnación de la prueba del hecho electrónico o de su manifestación tendrá como una de sus principales consecuencias la sujeción del medio probatorio a la libre valoración del juez o tribunal conforme a las reglas de la sana crítica. En este punto, el tribunal valorará la seriedad de los argumentos en que se fundamente la impugnación, así como los distintos medios de prueba instrumentales propuestos por las partes al objeto de acreditar o negar la realidad de los hechos. Evidentemente, la autenticidad e integridad de la prueba del hecho electrónico no quedará lo suficientemente en entredicho, al menos, como para carecer de valor probatorio, cuando la impugnación no se sustenta en ningún argumento concreto y la parte impugnante no ha tenido la diligencia de aportar medios de prueba que apoyen su impugnación. En este sentido, ARRABAL PLATERO, así como distintos autores, se han mostrado favorables a exigir un principio de prueba para admitir la impugnación de la autenticidad e integridad de la prueba del hecho electrónico, de forma que se den motivos, indicios o argumentos que hagan verosímil la impugnación[108].

Así pues, el valor probatorio de los documentos privados dependerá de la postura procesal de las partes y, más concretamente, de su impugnación o no[109]. De no

[107] A pesar de ello, se entiende que las previsiones de prueba tasada documental sí que serán de aplicación en la medida en que sean coherentes con las normas y principios que rigen el proceso penal.
[108] ARRABAL PLATERO, P. *La prueba tecnológica…*, ob. cit., 2020, págs. 341-352.
[109] Los documentos públicos, determinados documentos administrativos (artículo 319 LEC) y de los documentos privados cuando no se impugne su autenticidad (artículo 326 LEC) harán prueba plena del

efectuarse impugnación alguna, el documento impreso que contenga los mensajes de correo electrónico tendrá pleno valor probatorio de los extremos que contenga. Si se impugna la autenticidad y no se puede deducir su genuidad de la prueba propuesta o no se hubiere propuesto ninguna prueba, el juez o tribunal lo valorará conforme a las reglas de la sana crítica[110]. Sin embargo, no hay una postura única con relación al sistema de valoración que deba aplicarse cuando de la prueba instrumental practicada se deduzca su autenticidad, aunque parece razonable entender que probada la autenticidad de los documentos estos deben hacer prueba plena en los términos del artículo 319 LEC.

En lo que respecta a los documentos firmados electrónicamente, la eficacia probatoria de este tipo de documentos viene establecida en el artículo 3 LFE, aplicable en todos los órdenes jurisdiccionales. Con carácter general, el artículo 3.7 LFE determina que los documentos electrónicos regulados en el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de acuerdo con la legislación que les sea aplicable. En relación a los distintos tipos de firma, la norma solamente recoge una previsión relacionada con el valor probatorio de la firma electrónica reconocida, que será el mismo que el de la firma manuscrita (artículo 3.4 LFE). La firma electrónica avanzada y la firma electrónica común, por su parte, en cuanto a sus efectos jurídicos se regirán por lo previsto en el artículo 3.9 LFE, de modo que su eficacia será la propia del tipo de documento mediante el cual se incorporen al proceso. Asimismo, en concordancia con lo previsto para los documentos tradicionales, su valor probatorio se encuentra condicionado a la postura procesal de las partes

Finalmente, nada dice la LEC sobre la forma en que ha de valorarse el reconocimiento judicial, existiendo cierta discusión doctrinal acerca de su fuerza probatoria como prueba tasada o su sujeción a las reglas de la sana crítica.

---

hecho, acto o estado de las cosas que documenten, de la fecha en que tenga lugar esa documentación y de la identidad de los fedatarios y de las personas que, en su caso, hayan intervenido. De este modo, el acta notarial que aporte alguna de las partes hará prueba de los aspectos señalados, es decir, que en una fecha determinada un terminal contenía unos concretos mensajes de WhatsApp (y demás extremos apreciables por el notario), o que un disco duro contenía una información y datos concretos en dicho momento. Por el contrario, no quedará garantizada la autenticidad e integridad de los mensajes o del contenido del disco duro y, por otro lado, tampoco se impide que la realidad de los hechos alegados pueda desvirtuarse mediante prueba en contrario

[110] Así se desprende de la sentencia de la Audiencia Provincial de Lleida de 30/01/2014, núm. 51/2014 (Aranzadi).

3.3 Valoración conjunta de la prueba

Lo habitual en la práctica jurídica ante los tribunales será la coexistencia pruebas contradictorias y/o complementarias entre sí, por lo que la decisión del órgano judicial debe sustentarse en la valoración conjunta de todos los medios de prueba. La apreciación conjunta de la prueba, que es un sistema de valoración de creación jurisprudencial, consiste en comparar y confrontar el resultado obtenido en la práctica de los distintos medios de prueba[111].

Este sistema mixto de valoración ha sido criticado por parte de la doctrina al entender que permite sortear las reglas de valoración de la prueba (como la prueba tasada) y que puede mermar la motivación real de la sentencia, al carecer de una valoración individual y pormenorizada de cada una de las pruebas. A pesar de ello, no puede admitirse la exclusión de este sistema de valoración pues, como declara el Tribunal Supremo, aunque en ciertas ocasiones puede generar indefensión y hacer que la sentencia quede escasa de motivación, *«no cabe satanizar la valoración conjunta de la prueba, exponente del principio de libre valoración de la misma, cuando no resulta arbitraria, ilógica, contraria a derecho y no provoca indefensión»*[112]. De esta forma, la correcta práctica de la valoración en conjunto debe respetar las reglas de la valoración legal y de la libre valoración, debiendo efectuar una valoración individualizada de cada medio de prueba. En todo caso, es imprescindible cumplir con la exigencia constitucional de motivación de las sentencias (artículo 120.3 CE).

DE URBANO CASTRILLO explica de la siguiente manera las distintas etapas y la forma correcta de proceder en la valoración conjunta de la prueba[113]:

1) Juicio de admisibilidad: únicamente deben admitirse las pruebas que cumplan con los requisitos de licitud, pertinencia y utilidad.
2) Acervo probatorio: delimitar claramente qué pruebas serán objeto de valoración por el órgano judicial, diferenciando entre pruebas de cargo y de descargo.

[111] En este sentido, la sentencia de la Audiencia Provincial de Asturias de 29/07/2014, núm. 336/2014 (Aranzadi), que efectúa una apreciación conjunta de la declaración de parte, de la prueba pericial y de la prueba documental.
[112] Sentencia del Tribunal Supremo de 09/06/2010, núm. 334/2010 (Aranzadi).
[113] DE URBANO CASTRILLO, E. *La valoración de la prueba electrónica.* Tirant lo Blanch, Valencia, 2009 pág. 30.

3) Ponderación individualizada de cada prueba: en esta fase, de conformidad con las reglas de valoración legales y de la sana crítica, el órgano judicial otorgará un mayor o menor valor probatorio a cada uno de los medios de prueba.
4) Decisión: en esta última fase del proceso valorativo será fundamental el *iter* lógico seguido por el juez o tribunal para motivar la sentencia, con especial atención a la forma de resolver aquellas cuestiones que cuentan con pruebas contrarias entre sí.

La valoración conjunta de la prueba resultará más complicada cuando se deba lidiar con medios de prueba contradictorios unos con otros, lo cual plantea las siguientes posibilidades: — 1º confrontación entre medios probatorios de valor tasado; — 2º entre medios de prueba de libre valoración; y, — 3º entre medios de prueba tasada y de libre valoración. En el primero de los casos dado que se trata de pruebas que hacen prueba plena de los mismos aspectos el juez valorará de acuerdo con las reglas de la sana crítica. Piénsese en el caso de dos documentos públicos, un acta notarial y un acta levantada por el LAJ, que den fe de unos mensajes o de una página web cuyo contenido es diferente en uno y en otro. Misma solución se alcanza en la segunda de las situaciones, cuando se producen declaraciones de diferentes testigos contradictorias en relación a un mismo hecho o informes periciales con conclusiones divergentes. En el último caso, la situación se solventa declarando la prevalencia del valor probatorio de la prueba tasada sobre las sometidas a la libre valoración del órgano enjuiciador.

IV CONCLUSIONES

1. El hecho electrónico es un hecho relacionado mediata o inmediatamente con la electrónica, es decir, tiene relación con dispositivos que utilizan la electrónica. Con carácter general, lo que resulta de interés es el modo en el que la tecnología ofrece hechos susceptibles de ser captados por nuestros sentidos, ya sea mediante impresiones en papel, información ofrecida en pantallas de video u otras formas. La calificación de un hecho como electrónico no lo hace diferente del resto de hechos en general y, por tanto, no estará sujeto a exigencias legales distintas a efectos de conseguir su introducción en el proceso jurisdiccional ni tampoco en cuanto a su valoración.

2. La investigación forense y la obtención de la prueba del hecho electrónico se encuentran especialmente marcadas por el riesgo de superar los límites fijados por los

derechos fundamentales, cuya vulneración determina la ilicitud de la prueba. Con todo, existen claras diferencias en cuanto a las facultades de las partes para llevar a cabo la investigación de los hechos. Así, en el proceso civil, ante la ausencia de una regulación legal que permita una mayor capacidad de investigación, la investigación forense y la obtención de la prueba del hecho electrónico quedarán limitadas a aquello que le es accesible a la parte. En el proceso penal, por el contrario, no existe este problema y podrán llevarse a cabo las distintas diligencias de investigación tecnológica previstas en la LECrim siempre que se cumpla con los requisitos legales. En un punto intermedio se encuentra el proceso social, en el que podrá realizarse una adecuada investigación forense sobre los dispositivos electrónicos propiedad de la empresa siempre y cuando se cumplan determinados requisitos como el establecimiento de normas de uso, la información previa o los requisitos propios del procedimiento de investigación.

3. El hecho electrónico podrá introducirse en el proceso por cualquiera de los medios de prueba previstos en el artículo 299.1 y 2 LEC. En este sentido, la parte optará por uno u otro medio de prueba dependiendo de la naturaleza o manifestaciones del hecho y de aquello que se quiera probar. A estos efectos, será conveniente emplear distintos medios probatorios para reforzar la prueba del hecho electrónico con el fin de alcanzar el convencimiento del juez o tribunal. Por este motivo, en contra de lo que frecuentemente se afirma, no resulta imprescindible la aportación de una prueba pericial, sino que la necesidad de la misma vendrá condicionada por las circunstancias del caso, el conjunto de las pruebas de que se disponga y de la postura procesal de la parte contraria.

4. Nótese, además, que el ordenamiento jurídico procesal no contempla en ninguno de sus artículos un medio probatorio que pudiera corresponderse con la llamada “prueba electrónica”. Aquello que trascienda de nuestros sentidos, como, por ejemplo, datos digitales o radiaciones electromagnéticas, deberá probarse mediante prueba pericial que dé cuenta de los detalles técnicos del hecho electrónico no directamente aprehensibles por el ser humano. De esta forma, de admitirse la existencia de la prueba electrónica, la misma deberá situarse dentro de la prueba pericial como prueba pericial informática o tecnológica, sin que por ello pierda su naturaleza de prueba pericial.

5. Por último, la valoración de la prueba del hecho electrónico se regirá por el principio básico de la libre valoración en el marco de una valoración conjunta de los medios probatorios que permita al órgano judicial hacerse una imagen de la realidad de los hechos para dictar sentencia.

V BIBLIOGRAFÍA

ABEL LLUCH, X. Y PICÓ I JUNOY, J. *La prueba electrónica. Colección de Formación Continua Facultad de Derecho ESADE.* J.M. Bosch editor, Barcelona, 2011.

ARRABAL PLATERO, P. *La prueba tecnológica: aportación, práctica y valoración.* Tirant lo Blanch, Valencia, 2020.

BACHMAIER WINTER, L. "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", en *Boletín del Ministerio de Justicia*, nº2195, 2017.

BUENO DE MATA, F. *Prueba electrónica y proceso 2.0.* Tirant lo Blanch, Valencia, 2014.

BUENO DE MATA, F. Y GONZÁLEZ PULIDO, I. *Fodertics 7.0. Estudios sobre derecho digital.* Editorial Comares, Granada, 2019.

CAPEÁNS AMENEDO, C. *Derecho del trabajo y nuevas tecnologías. Conflicto entre las tecnologías de información y comunicación y el derecho a la intimidad y propia imagen.* Colex, A Coruña, 2020.

CORTÉS DOMÍNGUEZ, V. Y MORENO CATENA, V. *Derecho procesal civil parte general.* Tirant lo Blanch, Valencia, 2019.

DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones.* Wolters Kluwer, Madrid, 2016.

DELGADO MARTÍN, J. "La prueba del whatsapp", en *Diario La Ley*, núm. 8605, 2015.

DÍAZ MARTÍNEZ, M. Y LÓPEZ-BARAJAS PEREA, I. *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas.* Tirant Lo Blanch, Valencia, 2018.

DE URBANO CASTRILLO, E. *La valoración de la prueba electrónica.* Tirant lo Blanch, Valencia, 2009.

FERNÁNDEZ RODRÍGUEZ, J.J. "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional,* 108, 93-122.doi: http://dx.doi.org/10.18042/cepc/redc.108.03

GARCÍA MESCUA, D. *Aportación de mensajes WhatsApp a los procesos judiciales. Tratamiento procesal.* Comares, Granada, 2018.

GUARDIOLA SALMERÓN, M. (2018). ¿Cómo recabar y aportar la prueba digital? *Derecho & Perspectiva*, págs. 1-6. Recuperado de http://derechoyperspectiva.es/como-recabar-y-aportar-la-prueba-digital/

ILLAN FERNÁNDEZ, J.M., *La prueba electrónica, eficacia y valoración en el proceso civil. Nueva oficina judicial, comunicaciones telemáticas (Lexnet) y el expediente judicial electrónico. Análisis comparado legislativo y jurisprudencial.* Aranzadi, Navarra, 2009.

MONREAL BRINGSVAERD, E., THIBAULT ARANDA, X. Y JURADO SEGOVIA, A. *Derecho del trabajo y nuevas tecnologías. Estudios en homenaje al profesor Francisco Pérez de los Cobos Orihuel*, Tirant lo Blanch, Valencia, 2020.

ORMAZÁBAL SÁNCHEZ, G. *La prueba documental y la prueba mediante soportes informáticos*, Wolters Kluwer, Madrid, 2019.

RICHARD GONZÁLEZ, M. *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, Wolters Kluwer, Madrid, 2017.

RICHARD GONZÁLEZ, M. "Análisis crítico sobre la naturaleza y características de la prueba pericial electrónica en el proceso jurisdiccional", en *Revista Jurídica de Catalunya-Aranzadi*, 2017.

RICHARD GONZÁLEZ, M. "Investigación y prueba de hechos y dispositivos electrónicos", en *Revista General de Derecho Procesal*, 2017.

RICHARD GONZÁLEZ, M. "Requisitos y límites de la investigación preprocesal y prueba pericial sobre dispositivos electrónicos de la empresa usados por el empleado", en *Diario LA LEY*, 2017.

RICHARD GONZÁLEZ, M. "Reglas para la investigación forense y aportación como prueba al proceso de correos y mensajes electrónicos del trabajador (comentario a la STS sala cuarta de lo social, nº119/2018 de 8 feb. 2018, rec.1121/2015. LA LEY 4068/2018)", en *Diario LA LEY*, 2018.

SANCHÍS CRESPO, C. *La prueba en soporte electrónico,* en VALERO TORRIJOS, J. (coord.), *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio*, Thomson Reuters Aranzadi, Navarra, 2012.

PICÓ I JUNOY, J. ANDINO LÓPEZ, J.A. Y CERRATO GURI, E. *La prueba pericial a examen. Propuestas de lege ferenda*, Bosch, Barcelona, 2020.

PINTO PALACIOS, F. Y PUJOL CAPILLA, P. *La prueba en la era digital.* Wolters Kluwer, Madrid, 2017.

PINTO PALACIOS, F. Y PUJOL CAPILLA, P. "La prueba pericial informática", en *Diario La Ley*, núm. 5, 2017.

VEGAS TORRES, J. *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa* Universidad Rey Juan Carlos, Madrid, 2011

VI JURISPRUDENCIA

1) Tribunal Europeo de Derechos humanos

Sentencia del Tribunal Europeo de Derechos Humanos de 22/02/2018, Caso Libert contra Francia.

Sentencia del Tribunal Europeo de Derechos Humanos de 05/09/2017, Caso Barbulescu contra Rumania.

Sentencia del Tribunal Europeo de Derechos Humanos de 03/04/2007, Caso Copland contra Reino Unido.

Sentencia del Tribunal Europeo de Derechos Humanos de 02/08/1984, Caso Malone contra Reino Unido.

2) Tribunal Constitucional

Sentencia del Tribunal Constitucional de 15/03/2021, núm. rec. 6838/2019.

Sentencia del Tribunal Constitucional de 28/02/2019, núm. 25/2019.

Sentencia del Tribunal Constitucional de 09/05/2013, núm. 115/2013.

Sentencia del Tribunal Constitucional de 11/02/2013, núm. 29/2013.

Sentencia del Tribunal Constitucional de 02/07/2012, núm. 142/2012.

Sentencia del Tribunal Constitucional de 30/01/2012, núm.12/2012.

Sentencia del Tribunal Constitucional de 07/11/2011, núm. 173/2011.

Sentencia del Tribunal Constitucional de 09/10/2006, núm. 281/2006.

Sentencia del Tribunal Constitucional de 10/02/2003, núm. 22/2003.

Sentencia del Tribunal Constitucional de 03/06/2002, núm. 137/2002.

Sentencia del Tribunal Constitucional de 03/04/2002, núm. 70/2002.

Sentencia del Tribunal Constitucional de 30/11/2000, núm. 292/2000.

Sentencia del Tribunal Constitucional de 05/04/1999, núm. 49/1999.

Sentencia del Tribunal Constitucional de 29/11/1984, núm. 114/1984.

3) Tribunal Supremo

Sentencia del Tribunal Supremo de 23/07/2020, núm. 706/2020.

Sentencia del Tribunal Supremo de 07/05/2020, núm. 135/2020.

Sentencia del Tribunal Supremo de 08/05/2019, núm. 347/2019.

Sentencia del Tribunal Supremo de 07/02/2019, núm. 65/2019.

Sentencia del Tribunal Supremo de 19/07/2018, núm. 375/2018.

Sentencia del Tribunal Supremo de 08/02/2018, núm. 119/2018.

Sentencia del Tribunal Supremo de 19/04/2017, núm. 287/2017.

Sentencia del Tribunal Supremo de 13/04/2016, núm. 307/2016.

Sentencia del Tribunal Supremo de 10/03/2016, núm. 204/2016.

Sentencia del Tribunal Supremo de 04/12/2015, núm. 786/2015.

Sentencia del Tribunal Supremo de 19/05/2015, núm. 300/2015.

Sentencia del Tribunal Supremo de 04/02/2015, núm. 23/2015.

Sentencia del Tribunal Supremo de 06/10/2011, núm. rec. 4053/2010

Sentencia del Tribunal Supremo de 08/07/2011, núm. rec. 6115/2007.

Sentencia del Tribunal Supremo de 09/06/2010, núm. 334/2010.

Sentencia del Tribunal Supremo de 26/09/2007, núm. rec. 966/2006.

Sentencia del Tribunal Supremo de 30/04/2007, núm. 357/2007 (Aranzadi).

Sentencia del Tribunal Supremo de 07/12/2001, núm. 2384/2001.

4) Tribunal Superior de Justicia

Sentencia del Tribunal Superior de Justicia de Andalucía de 17/06/2020, núm. 1629/2020.

Sentencia del Tribunal Superior de Justicia de Galicia de 05/06/2020, núm. rec. 3815/2019.

Sentencia del Tribunal Superior de Justicia de Madrid de 19/07/2019, núm. 804/2019.

Sentencia del Tribunal Superior de Justicia de Andalucía de 28/03/2019, núm. 905/2019.

Sentencia del Tribunal Superior de Justicia de Madrid de 05/05/2017, núm. 313/2017.

Sentencia del Tribunal Superior de Justicia de Madrid de 13/05/2016, núm. 407/2016.

Sentencia del Tribunal Superior de Justicia de Galicia de 28/01/2016, núm. 556/2016.

Sentencia del Tribunal Superior de Justicia de Madrid de 21/03/2014, núm. 260/2014.

Sentencia del Tribunal Superior de Justicia de Cataluña de 05/05/2011, núm. 11/2011.

5) Audiencia Provincial

Sentencia de la Audiencia Provincial de Barcelona de 17/09/2020, núm. 614/2020.

Sentencia de la Audiencia Provincial de Alicante de 10/04/2019, núm. 142/2019.

Sentencia de la Audiencia Provincial de Madrid de 20/11/2017, núm. 291/2017.

Sentencia de la Audiencia Provincial de Barcelona de 06/09/2016, núm. 486/2016.

Sentencia de la Audiencia Provincial de Asturias de 29/07/2014, núm. 336/2014.

Sentencia de la Audiencia Provincial de Córdoba de 02/04/2014, núm. 159/2014.

Sentencia de la Audiencia Provincial de Lleida de 30/01/2014, núm. 51/2014.

Sentencia de la Audiencia Provincial de Madrid de 01/10/2012, núm. 1260/2012.

6) Juzgados

Sentencia del Juzgado de lo Mercantil nº8 de Barcelona de 16/12/2019, núm. 291/2019.

Sentencia del Juzgado de lo Social nº3 de Pamplona de 31/03/2017, núm. 74/2017.